Bitdefender®

TOTAL SECURITY 2016

USER'S GUIDE

Bitdefender Total Security 2016
User's Guide

Publication date 09/23/2015

Copyright© 2015 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Bitdefender

Table of Contents

Installation 1

1. Preparing for installation 2

2. System requirements 3
   2.1. Minimum system requirements 3
   2.2. Recommended system requirements 3
   2.3. Software requirements 4

3. Installing your Bitdefender product 5
   3.1. Install from Bitdefender Central 5
   3.2. Install from installation disc 8

Getting started 12

4. The basics 13
   4.1. Opening the Bitdefender window 13
   4.2. Fixing issues 14
      4.2.1. Fix all Issues wizard 15
      4.2.2. Configuring status alerts 16
   4.3. Events 16
   4.4. Autopilot 17
   4.5. Profiles and Battery Mode 18
      4.5.1. Profiles 19
      4.5.2. Battery Mode 20
   4.6. Password-protecting Bitdefender settings 21
   4.7. Anonymous usage reports 22
   4.8. Special offers and product notifications 23

5. Bitdefender interface 24
   5.1. System tray icon 24
   5.2. Main window 25
      5.2.1. Upper toolbar 26
      5.2.2. Action buttons 27
   5.3. The Bitdefender modules 28
      5.3.1. **Protection** 28
      5.3.2. **Privacy** 29
      5.3.3. **Tools** 31
   5.4. Security Widget 32
      5.4.1. Scanning files and folders 33
      5.4.2. Hide / show Security Widget 33
   5.5. Security Report 34
      5.5.1. Checking the Security Report 36
      5.5.2. Turning on or off the Security Report notification 36

6. Bitdefender Central 38
   6.1. Accessing your Bitdefender Central account 38
   6.2. My Subscriptions 39

6.2.1. Check available subscriptions . . . 39
6.2.2. Add a new device . . . 39
6.2.3. Renew subscription . . . 40
6.2.4. Activate subscription . . . 40
6.3. My Devices . . . 40

7. Keeping Bitdefender up-to-date . . . 43
7.1. Checking if Bitdefender is up-to-date . . . 43
7.2. Performing an update . . . 44
7.3. Turning on or off automatic update . . . 44
7.4. Adjusting update settings . . . 45

How to . . . 47

8. Installation . . . 48
8.1. How do I install Bitdefender on a second computer? . . . 48
8.2. When should I reinstall Bitdefender? . . . 48
8.3. Where can I download my Bitdefender product from? . . . 49
8.4. How do I use my Bitdefender subscription after a Windows upgrade? . . . 49
8.5. How do I repair Bitdefender? . . . 52

9. Subscriptions . . . 54
9.1. What Bitdefender product am I using? . . . 54
9.2. How do I activate Bitdefender subscription using a license key? . . . 54

10. Bitdefender Central . . . 56
10.1. How do I log in to Bitdefender Central using another online account? . . . 56
10.2. How do I reset the password for Bitdefender Central account? . . . 56

11. Scanning with Bitdefender . . . 58
11.1. How do I scan a file or a folder? . . . 58
11.2. How do I scan my system? . . . 58
11.3. How do I schedule a scan? . . . 58
11.4. How do I create a custom scan task? . . . 59
11.5. How do I exclude a folder from being scanned? . . . 60
11.6. What to do when Bitdefender detected a clean file as infected? . . . 61
11.7. How do I check what viruses Bitdefender detected? . . . 62

12. Parental Advisor . . . 63
12.1. How do I protect my children from online threats? . . . 63
12.2. How do I block my child's access to a website? . . . 64
12.3. How do I prevent my child from playing a game? . . . 64
12.4. How do I prevent my child from getting in contact with untrusted persons? . . . 65
12.5. How can I set a location as safe or restricted for my child? . . . 66
12.6. How do I create Windows user accounts? . . . 67
12.7. How to remove a child profile . . . 68

13. Privacy protection . . . 69
13.1. How do I make sure my online transaction is secure? . . . 69
13.2. What can I do if my device has been stolen? . . . 69
13.3. How do I use file vaults? . . . 70
13.4. How do I remove a file permanently with Bitdefender? . . . 71

14. Tune-Up 73
14.1. How do I improve my system performance? 73
14.1.1. Optimize your system performance with a single click 73
14.1.2. Scan your system periodically 73
14.2. How can I improve my system startup time? 74
15. Useful Information 75
15.1. How do I test my antivirus solution? 75
15.2. How do I remove Bitdefender? 75
15.3. How do I automatically shut down the computer after the scan is over? 76
15.4. How do I configure Bitdefender to use a proxy Internet connection? 77
15.5. Am I using a 32 bit or a 64 bit version of Windows? 78
15.6. How do I display hidden objects in Windows? 79
15.7. How do I remove other security solutions? 80
15.8. How do I restart in Safe Mode? 81
Managing your security 82
16. Antivirus protection 83
16.1. On-access scanning (real-time protection) 84
16.1.1. Turning on or off real-time protection 84
16.1.2. Adjusting the real-time protection level 85
16.1.3. Configuring the real time protection settings 85
16.1.4. Restoring the default settings 89
16.2. On-demand scanning 89
16.2.1. Scanning a file or folder for malware 89
16.2.2. Running a Quick Scan 90
16.2.3. Running a System Scan 90
16.2.4. Configuring a custom scan 91
16.2.5. Antivirus Scan Wizard 94
16.2.6. Checking scan logs 97
16.3. Automatic scan of removable media 97
16.3.1. How does it work? 98
16.3.2. Managing removable media scan 99
16.4. Configuring scan exclusions 99
16.4.1. Excluding files or folders from scanning 100
16.4.2. Excluding file extensions from scanning 100
16.4.3. Managing scan exclusions 101
16.5. Managing quarantined files 102
16.6. Active Threat Control 103
16.6.1. Checking detected applications 103
16.6.2. Turning on or off Active Threat Control 104
16.6.3. Adjusting the Active Threat Control protection 104
16.6.4. Managing excluded processes 104
17. Antispam 106
17.1. Antispam insights 107
17.1.1. Antispam filters 107
17.1.2. Antispam operation 107
17.1.3. Supported e-mail clients and protocols 108

17.2. Turning on or off antispam protection ... 108
17.3. Using the antispam toolbar in your mail client window ... 108
17.3.1. Indicating detection errors ... 109
17.3.2. Indicating undetected spam messages ... 110
17.3.3. Configuring toolbar settings ... 110
17.4. Configuring the Friends List ... 111
17.5. Configuring the Spammers List ... 112
17.6. Configuring the local antispam filters ... 113
17.7. Configuring the cloud settings ... 114

18. Web Protection ... 115
18.1. Bitdefender alerts in the browser ... 116

19. Data protection ... 117
19.1. Deleting files permanently ... 117

20. File encryption ... 118
20.1. Managing file vaults ... 118
20.2. Creating file vaults ... 118
20.3. Opening file vaults ... 119
20.4. Adding files to vaults ... 120
20.5. Locking vaults ... 120
20.6. Removing files from vaults ... 121
20.7. Changing vault password ... 121

21. Vulnerability ... 123
21.1. Scanning your system for vulnerabilities ... 123
21.2. Using automatic vulnerability monitoring ... 124

22. Firewall ... 127
22.1. Turning on or off firewall protection ... 127
22.2. Managing firewall rules ... 128
22.2.1. General rules ... 128
22.2.2. Application rules ... 129
22.3. Managing connection settings ... 131
22.4. Configuring advanced settings ... 133
22.5. Configuring alert intensity ... 133

23. Intrusion Detection ... 135

24. Ransomware Protection ... 136
24.1. Turning on or off Ransomware Protection ... 136
24.2. Protect personal files from ransomware attacks ... 137
24.3. Configuring trusted applications ... 137
24.4. Configuring blocked applications ... 137
24.5. Protection at boot ... 138

25. Safepay security for online transactions ... 139
25.1. Using Bitdefender Safepay™ ... 140
25.2. Configuring settings ... 141
25.3. Managing bookmarks ... 142
25.4. Hotspot protection for unsecured networks ... 142

26. Password Manager protection for your credentials 144
26.1. Configuring the Password Manager 145
26.2. Turning on or off the Password Manager protection 148
26.3. Managing the Password Manager settings 148
27. Parental Advisor 152
27.1. Accessing Parental Advisor - My Children 152
27.2. Adding your child's profile 153
27.2.1. Linking Parental Advisor to Bitdefender Central 154
27.2.2. Monitoring the child's activity 154
27.2.3. Configuring the General Settings 155
27.2.4. Editing a profile 156
27.2.5. Removing a profile 156
27.3. Configuring Parental Advisor profiles 156
27.3.1. Timeline 157
27.3.2. Activities 157
27.3.3. Interests 158
27.3.4. Friends 158
27.3.5. Places 159
27.3.6. Social 160
28. Device Anti-Theft 161
29. USB Immunizer 163
System optimization 164
30. Tune-Up 165
30.1. Optimizing your system speed with a single click 165
30.2. Optimizing your PC's boot time 166
31. Profiles 168
31.1. Work Profile 169
31.2. Movie Profile 170
31.3. Game Profile 171
31.4. Real-Time Optimization 172
Troubleshooting 174
32. Solving common issues 175
32.1. My system appears to be slow 175
32.2. Scan doesn't start 176
32.3. I can no longer use an application 179
32.4. What to do when Bitdefender blocks a safe website or online application 180
32.5. I cannot connect to the Internet 181
32.6. I cannot access a device on my network 181
32.7. My Internet is slow 183
32.8. How to update Bitdefender on a slow Internet connection 184
32.9. My computer is not connected to the Internet. How do I update Bitdefender? 185
32.10. Bitdefender services are not responding 185

32.11. Antispam filter does not work properly . . . 186
32.11.1. Legitimate messages are marked as [spam] . . . 186
32.11.2. Many spam messages are not detected . . . 188
32.11.3. Antispam filter does not detect any spam message . . . 190
32.12. The Autofill feature in my Wallet doesn't work . . . 191
32.13. Bitdefender removal failed . . . 192
32.14. My system doesn't boot up after installing Bitdefender . . . 193
33. Removing malware from your system . . . 196
33.1. Bitdefender Rescue Mode . . . 196
33.2. What to do when Bitdefender finds viruses on your computer? . . . 198
33.3. How do I clean a virus in an archive? . . . 199
33.4. How do I clean a virus in an e-mail archive? . . . 200
33.5. What to do if I suspect a file as being dangerous? . . . 201
33.6. What are the password-protected files in the scan log? . . . 202
33.7. What are the skipped items in the scan log? . . . 202
33.8. What are the over-compressed files in the scan log? . . . 203
33.9. Why did Bitdefender automatically delete an infected file? . . . 203
Contact us . . . 204
34. Asking for help . . . 205
35. Online resources . . . 207
35.1. Bitdefender Support Center . . . 207
35.2. Bitdefender Support Forum . . . 207
35.3. HOTforSecurity Portal . . . 208
36. Contact information . . . 209
36.1. Web addresses . . . 209
36.2. Local distributors . . . 209
36.3. Bitdefender offices . . . 209
Glossary . . . 212

INSTALLATION

1. PREPARING FOR INSTALLATION

Before you install Bitdefender Total Security 2016, complete these preparations to ensure the installation will go smoothly:

- Make sure that the computer where you plan to install Bitdefender meets the minimum system requirements. If the computer does not meet all the minimum system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, please refer to "*System requirements*" (p. 3).
- Log on to the computer using an Administrator account.
- Remove any other similar software from the computer. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled during the installation.
- Disable or remove any firewall program that may be running on the computer. Running two firewall programs simultaneously may affect their operation and cause major problems with the system. Windows Firewall will be disabled during the installation.
- It is recommended that your computer be connected to the Internet during the installation, even when installing from a CD/DVD. If newer versions of the application files included in the installation package are available, Bitdefender can download and install them.

2. SYSTEM REQUIREMENTS

You may install Bitdefender Total Security 2016 only on computers running the following operating systems:

- Windows 7 with Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Before installation, make sure that your computer meets the minimum system requirements.

Note

To find out the Windows operating system your computer is running and hardware information, follow these steps:

- In **Windows 7**, right-click **My Computer** on the desktop and then select **Properties** from the menu.
- In **Windows 8 and Windows 8.1**, from the Windows Start screen, locate Computer (for example, you can start typing "Computer" directly in the Start screen) and then right-click its icon. Select Properties in the bottom menu. Look in the System area to find information about your system type.
- In **Windows 10**, type "System" in the search box from the taskbar and click its icon. Look in the System area to find information about your system type.

2.1. Minimum system requirements

- 1 GB available free hard disk space (at least 800 MB on the system drive)
- 1.6 GHz processor
- 1 GB of memory (RAM)

2.2. Recommended system requirements

- 2 GB available free hard disk space (at least 800 MB on the system drive)
- Intel CORE Duo (2 GHz) or equivalent processor
- 2 GB of memory (RAM)

2.3. Software requirements

To be able to use Bitdefender and all its features, your computer needs to meet the following software requirements:

- Internet Explorer 10 or higher
- Mozilla Firefox 14 or higher
- Google Chrome 20 or higher
- Skype 6.3 or higher
- Yahoo! Messenger 9 or higher
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express and Windows Mail (on 32-bit systems)
- Mozilla Thunderbird 14 or higher

3. INSTALLING YOUR BITDEFENDER PRODUCT

You can install Bitdefender from the installation disc, or using the web installer downloaded on your computer from the Bitdefender Central account.

If your purchase covers more than one computer (for example, you purchased Bitdefender Total Security 2016 for 3 PCs), repeat the installation process and activate your product with the same account on every computer. The account you need to use is the one which contains your Bitdefender active subscription.

3.1. Install from Bitdefender Central

From the Bitdefender Central account you can download the installation kit corresponding to the purchased subscription. Once the installation process is complete, Bitdefender Total Security 2016 is activated.

To download Bitdefender Total Security 2016 from your Bitdefender Central account, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. In the **My Devices** window, click **INSTALL Bitdefender**.
4. Choose **Windows**, then choose one of the two available options:
   - I want to install Bitdefender **On this device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list, then click **Download** to continue.
   - I want to install Bitdefender **On another device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.
5. Wait for the download to complete, then run the installer.

Validating the installation

Bitdefender will first check your system to validate the installation.

If your system does not meet the minimum requirements for installing Bitdefender, you will be informed of the areas that need improvement before you can proceed.

If an incompatible antivirus program or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on. You may need to reboot your computer to complete the removal of detected antivirus programs.

The Bitdefender Total Security 2016 installation package is constantly updated. Click **Yes** when prompted in order to allow Bitdefender to download the files, ensuring you are installing the very latest version of the software.

Note
Downloading the installation files can take a long time, especially over slower Internet connections.

Once the installation is validated, the setup wizard will appear. Follow the steps to install Bitdefender Total Security 2016.

Step 1 - Bitdefender installation

The Bitdefender installation screen lets you choose what type of installation you want to perform.

For a completely hassle-free installation experience, just click the **Install** button. Bitdefender will be installed in the default location with default settings and you will skip directly to Step 3 of the wizard.

If you wish to configure the installation settings, click **Custom**.

Two additional tasks can be performed at this step:

- Please read the End User License Agreement before proceeding with the installation. The License Agreement contains the terms and conditions under which you may use Bitdefender Total Security 2016.

  If you do not agree to these terms, close the window. The installation process will be abandoned and you will exit setup.

- Enable sending **Anonymous Usage Reports**. By enabling this option, reports containing information about how you use the product are sent to the Bitdefender servers. This information is essential for improving the product and can help us provide a better experience in the future. Please note that these reports contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

Step 2 - Customize installation settings

> **Note**
> This step appears only if you have chosen to customize the installation during the previous step.

The following options are available:

Install path

By default, Bitdefender Total Security 2016 will be installed in C:\Program Files\Bitdefender\Bitdefender 2016\. If you want to change the installation path, click **Change** and select the folder in which you would like Bitdefender to be installed.

Configure proxy settings

Bitdefender Total Security 2016 requires access to the Internet for product registration, downloading security and product updates, in-cloud detection components, etc. If you use a proxy connection instead of a direct Internet connection, you must select this option and configure the proxy settings.

The settings can be imported from the default browser or you can enter them manually.

Click **Install** to confirm your preferences and begin the installation. If you change your mind, click the corresponding **Use default** button.

Step 3 - Installation in progress

Wait for the installation to complete. Detailed information about the progress is displayed.

Critical areas on your system are scanned for viruses, the latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.

Step 4 - Installation completed

Your Bitdefender product is successfully installed.

A summary of the installation is displayed. If any active malware was detected and removed during the installation, a system reboot may be required. Click **OK** to continue.

Step 5 - Get started

In the Get started window you can see the validity of your subscription.

Two additional tasks can be performed at this step:

- Buy a new subscription - this link redirects you to the Bitdefender page from where you can buy a new subscription.
- I have an activation code - this link redirects you to your Bitdefender Central account. Click **ACTIVATION CODE** in the My Subscription window that appears. Type the activation code you have, then click **SUBMIT**.

Click **Finish** to access the Bitdefender Total Security 2016 interface.

3.2. Install from installation disc

To install Bitdefender from the installation disc, insert the disc in the optical drive.

A installation screen should be displayed in a few moments. Follow the instructions to start installation.

> **Note**
>
> The installation screen provides an option to copy the installation package from the installation disc to a USB storage device. This is useful if you need to install Bitdefender on a computer that does not have a disc drive (for example, on a netbook). Insert the storage device into the USB drive and then click **Copy to USB**. Afterwards, go to the computer without a disc drive, insert the storage device into the USB drive and double-click runsetup.exe from the folder where you have saved the installation package.

If the installation screen does not appear, use Windows Explorer to browse to the disc's root directory and double-click the file autorun.exe.

Validating the installation

Bitdefender will first check your system to validate the installation.

If your system does not meet the minimum requirements for installing Bitdefender, you will be informed of the areas that need improvement before you can proceed.

If an incompatible antivirus program or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow

the directions to remove the software from your system, thus avoiding problems occurring later on. You may need to reboot your computer to complete the removal of detected antivirus programs.

The Bitdefender Total Security 2016 installation package is constantly updated. Click **Yes** when prompted in order to allow Bitdefender to download the files, ensuring you are installing the very latest version of the software.

Note
Downloading the installation files can take a long time, especially over slower Internet connections.

Once the installation is validated, the setup wizard will appear. Follow the steps to install Bitdefender Total Security 2016.

Step 1 - Bitdefender Installation

The Bitdefender Installation screen lets you choose what type of installation you want to perform.

For a completely hassle-free installation experience, just click the **Install** button. Bitdefender will be installed in the default location with default settings and you will skip directly to Step 3 of the wizard.

If you wish to configure the installation settings, click **Custom**.

Two additional tasks can be performed at this step:

- Read the End User License Agreement before proceeding with the installation. The License Agreement contains the terms and conditions under which you may use Bitdefender Total Security 2016.

  If you do not agree to these terms, close the window. The installation process will be abandoned and you will exit setup.

- Select **Send anonymous usage reports**. By enabling this option, reports containing information about how you use the product are sent to the Bitdefender servers. This information is essential for improving the product and can help us provide a better experience in the future. Note that these reports contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

Step 2 - Customize installation settings

> **Note**
> This step appears only if you have chosen to customize the installation during the previous step.

The following options are available:

Install path

By default, Bitdefender Total Security 2016 will be installed in C:\Program Files\Bitdefender\Bitdefender 2016\. If you want to change the installation path, click **Change** and select the folder in which you would like Bitdefender to be installed.

Configure proxy settings

Bitdefender Total Security 2016 requires access to the Internet for product activation, downloading security and product updates, in-cloud detection components, etc. If you use a proxy connection instead of a direct Internet connection, you must select this option and configure the proxy settings.

The settings can be imported from the default browser or you can enter them manually.

Click **Install** to confirm your preferences and begin the installation. If you change your mind, click the corresponding **Use default** button.

Step 3 - Installation in progress

Wait for the installation to complete. Detailed information about the progress is displayed.

Critical areas on your system are scanned for viruses, the latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.

Step 4 - Installation completed

A summary of the installation is displayed. If any active malware was detected and removed during the installation, a system reboot may be required. Click **OK** to continue.

Step 5 - Bitdefender Central

After you complete the initial setup, the Bitdefender Central window appears. A Bitdefender Central account is required in order to activate the product and use its online features. For more information, please refer to "*Bitdefender Central*" (p. 38).

Proceed according to your situation.

I already have a Bitdefender Central account

Type the e-mail address and the password of your Bitdefender Central account, then click **SIGN IN**.

If you forgot the password for your account or you simply want to reset the one you already set, click the **Password reset** link. Type your e-mail address, then click the **RESET PASSWORD** button.

I want to create a Bitdefender Central account

To successfully create a Bitdefender Central account, click the **Sign Up** link located on the lower part of the window. Type the required information in the corresponding fields, and then click the **CREATE ACCOUNT** button.

The data you provide here will remain confidential.

The password must be at least 8 characters long and include a digit.

Note

Once the account is created, you can use the provided e-mail address and password to log in to your account at https://central.bitdefender.com.

Step 6 - Get started

In the Get started window you can see the validity of your subscription.

Two additional tasks can be performed at this step:

- Buy a new subscription - this link redirects you to the Bitdefender page from where you can buy a new subscription.
- I have an activation code - this link redirects you to your Bitdefender Central account. Click **ACTIVATION CODE** in the My Subscription window that appears. Type the code you have, then click **SUBMIT**.

Click **Finish** to access the Bitdefender Total Security 2016 interface.

GETTING STARTED

4. THE BASICS

Once you have installed Bitdefender Total Security 2016, your computer is protected against all kinds of malware (such as viruses, spyware and trojans) and Internet threats (such as hackers, phishing and spam).

The application uses the Photon technology to enhance the speed and performance of the anti-malware scanning process. It works by learning the usage patterns of your system applications to know what and when to scan, thus minimizing the impact on system performance.

You can engage the Autopilot to enjoy completely silent security and you are not required to configure any settings. However, you may want to take advantage of the Bitdefender settings to fine-tune and improve your protection.

While you work, play games or watch movies, Bitdefender can offer you a continuous user experience by postponing maintenance tasks, eliminating interruptions and adjusting system visual effects. You can benefit from all these by activating and configuring Profiles.

Bitdefender will make most security-related decisions for you and will rarely show pop-up alerts. Details about actions taken and information about program operation are available in the Events window. For more information, please refer to "*Events*" (p. 16).

From time to time, you should open Bitdefender and fix the existing issues. You may have to configure specific Bitdefender components or take preventive actions to protect your computer and your data.

To use the online features of Bitdefender Total Security 2016 and manage your subscriptions and devices, access your Bitdefender Central account. For more information, please refer to "*Bitdefender Central*" (p. 38).

The "How to" (p. 47) section is where you will find step-by-step instructions on how to perform common tasks. If you experience issues while using Bitdefender, check the "*Solving common issues*" (p. 175) section for possible solutions to the most common problems.

4.1. Opening the Bitdefender window

To access the main interface of Bitdefender Total Security 2016, follow the steps below:

- In **Windows 7**:
  1. Click **Start** and go to **All Programs**.
  2. Click **Bitdefender 2016**.
  3. Click **Bitdefender Total Security 2016** or, quicker, double-click the Bitdefender icon in the system tray.
- In **Windows 8 and Windows 8.1**:

  Locate Bitdefender Total Security 2016 from the Windows Start screen (for example, you can start typing "Bitdefender" directly in the Start screen) and then click its icon. Alternatively, open the Desktop app and then double-click the Bitdefender icon in the system tray.
- In **Windows 10**:

  Type "Bitdefender" in the search box from the taskbar and then click its icon. Alternatively, double-click the Bitdefender icon in the system tray.

For more information about the Bitdefender window and icon in the system tray, please refer to "*Bitdefender interface*" (p. 24).

4.2. Fixing issues

Bitdefender uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. By default, it will monitor only a series of issues that are considered to be very important. However, you can configure it as needed, choosing which specific issues you want to be notified about.

Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. They are grouped into two categories:

- **Critical issues** - prevent Bitdefender from protecting you against malware or represent a major security risk.
- **Minor (non-critical) issues** - can affect your protection in the near future.

The Bitdefender icon in the system tray indicates pending issues by changing its color as follows:

Critical issues are affecting the security of your system. They require your immediate attention and must be fixed as soon as possible.

Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.

Also, if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.

When you open the Bitdefender interface, the Security status area on the upper toolbar will indicate nature of issues affecting your system.

4.2.1. Fix all Issues wizard

To fix detected issues follow the **Fix all issues** wizard.

1. To open the wizard, do any of the following:
   - Right-click the Bitdefender icon in the system tray and choose **View security issues**.
   - Open the Bitdefender interface and click anywhere inside the Security status area on the upper toolbar (for example, you can click the **Fix all issues!** link).
2. You can see the issues affecting the security of your computer and data. All current issues are selected to be fixed.

   If you do not want to fix a specific issue right away, clear the corresponding check box. You will be prompted to specify for how long to postpone fixing the issue. Choose the desired option from the menu and click **OK**. To stop monitoring the respective issue category, choose **Permanently**.

   The issue status will change to **Postponed** and no action will be taken to fix the issue.
3. To fix the selected issues, click **Fix**. Some issues are fixed immediately. For others, a wizard helps you fix them.

The issues that this wizard helps you fix can be grouped into these main categories:

- **Disabled security settings.** Such issues are fixed immediately, by enabling the respective security settings.
- **Preventive security tasks you need to perform.** When fixing such issues, a wizard helps you successfully complete the task.

4.2.2. Configuring status alerts

Bitdefender can inform you when issues are detected in the operation of the following program components:

- Firewall
- Antispam
- Antivirus
- Update
- Browser Security

You can configure the alert system to best serve your security needs by choosing which specific issues to be informed about. Follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **Advanced** tab.
3. Click the **Configure status alerts** link.
4. Click the switches to turn on or off status alerts according to your preferences.

4.3. Events

Bitdefender keeps a detailed log of events concerning its activity on your computer. Whenever something relevant to the security of your system or data happens, a new message is added to the Bitdefender Events, in a similar way to a new e-mail appearing in your Inbox.

Events are a very important tool in monitoring and managing your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if malware was found on your computer etc. Additionally, you can take further action if needed or change actions taken by Bitdefender.

To access the Events log, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.

Messages are grouped according to the Bitdefender module whose activity they are related to:

- **Update**

- **Antivirus**
- **Web Protection**
- **Vulnerability**
- **Firewall**
- **Intrusion Detection**
- **Antispam**
- **Ransomware Protection**
- **File Encryption**
- **Tune-Up**

Every time an event occurs, a dot can be noticed on the icon at the top of the Bitdefender interface.

A list of events is available for each category. To find out information about a particular event in the list, click the icon and select **Events** from the drop-down menu. Event details are displayed in the right side of the window. Each event comes with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. Options may be provided to take further action if needed.

You can filter events by their importance and in the order they happened. There are three types of events filtered by their importance, each type indicated by a specific icon:

- **Critical** events indicate critical issues. You should check them immediately.
- **Warning** events indicate non-critical issues. You should check and fix them when you have the time.
- **Information** events indicate successful operations.

To view the events that occurred in a period of time, select the desired period from the corresponding field.

To help you easily manage logged events, each section of the Events window provides options to delete or mark as read all events in that section.

4.4. Autopilot

For all the users who want nothing more from their security solution than to be protected without being bothered, Bitdefender Total Security 2016 has been designed with a built-in Autopilot mode.

While on Autopilot, Bitdefender applies an optimal security configuration and takes all security-related decisions for you. This means you will see no pop-ups, no alerts and you will not have to configure any settings whatsoever.

In Autopilot mode, Bitdefender automatically fixes critical issues, enables and quietly manages:

- Antivirus protection, provided by on-access scanning and continuous scanning.
- Firewall protection.
- Web Protection.
- Automatic updates.

To turn the Autopilot on or off, follow these steps:

1. Click the **Autopilot** switch on the upper toolbar of the Bitdefender interface.

As long as the Autopilot is on, the Bitdefender icon in the system tray changes to B.

Important
While the Autopilot is on, modifying any of the settings it manages will result in it being turned off.

To see a history of actions performed by Bitdefender while Autopilot was engaged, open the Events window.

4.5. Profiles and Battery Mode

Some computer activities, such as online games or video presentations, require increased system responsiveness, high performance and no interruptions. When your laptop is running on battery power, it is best that unnecessary operations, which consume additional power, be postponed until the laptop is connected back to A/C power.

To adapt to these particular situations, Bitdefender Total Security 2016 includes two special operation modes:

- Profiles
- Battery Mode

4.5.1. Profiles

Bitdefender Profiles assigns more system resources to the running applications by temporarily modifying protection settings and adjusting system configuration. Consequently, the system impact on your activity is minimized.

To adapt to different activities, Bitdefender comes with the following profiles:

Work Profile
: Optimizes your work efficiency by identifying and adjusting the product and system settings.

Movie Profile
: Enhances visual effects and eliminates interruptions when watching movies.

Game Profile
: Enhances visual effects and eliminates interruptions when playing games.

Turning on or off profiles

To turn on or off profiles, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module.
4. In the **Profiles** window, select the **Profiles Settings** tab.
5. Turn on or off profiles by clicking the corresponding switch.

Configure Autopilot to monitor profiles

For an easy-to-use user experience, you can configure Autopilot to manage your working profile. While in this mode, Bitdefender automatically detects the activity you perform and applies system and product optimization settings.

To allow Autopilot manage profiles, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.

3. Click the **Profiles** module.
4. In the **Profiles** window, select the **Profiles Settings** tab.
5. Check the corresponding **Let Autopilot manage my profiles** box.

If you do not want to let your Profile be automatically managed, leave the box unchecked and manually choose it from the **PROFILE** drop-down list from the Bitdefender interface.

For more information on Profiles, please refer to "*Profiles*" (p. 168)

4.5.2. Battery Mode

Battery Mode is specially designed for laptop and tablet users. Its purpose is to minimize both system and Bitdefender impact on power consumption when the battery charge level is lower than you select.

The following product settings are applied when Bitdefender operates in Battery Mode:

- Bitdefender Automatic Update is postponed.
- Scheduled scans are postponed.
- Security Widget is turned off.

Bitdefender detects when your laptop has switched to battery power and based on the battery charge level it automatically enters Battery Mode. Likewise, Bitdefender automatically exits Battery Mode when it detects the laptop is no longer running on battery.

To turn on or off Battery mode, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module, then select the **Battery Mode** tab.
4. Turn on or off automatic Battery Mode by clicking the corresponding switch.

   Drag the corresponding slider along the scale to set when the system should start operating in Battery Mode. By default, the mode is activated when the battery charge level drops below 30%.

Note
The Battery Mode is enabled by default on laptops and tablets.

Configuring Battery Mode

To configure Battery mode, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module, then select the **Battery Mode** tab.
4. Enable the feature by clicking the corresponding switch.
5. Click the **Configure** button.
6. Choose the system adjustments to be applied by checking the following options:
   - Optimize product settings for Battery Mode.
   - Postpone background programs and maintenance tasks.
   - Postpone Windows Automatic Updates.
   - Adjust power plan settings for Battery Mode.
   - Disable external devices and network ports.
7. Click **Save** to save the changes and close the window.

4.6. Password-protecting Bitdefender settings

If you are not the only person with administrative rights using this computer, it is recommended that you protect your Bitdefender settings with a password.

To configure password protection for the Bitdefender settings, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **General Settings** tab.
3. Turn on Password protection by clicking the corresponding switch.

4. Enter the password in the two fields and then click **OK**. The password must be at least 8 characters long.

Once you have set a password, anyone trying to change the Bitdefender settings will first have to provide the password.

Important

Be sure to remember your password or keep a record of it in a safe place. If you forget the password, you will have to reinstall the program or to contact Bitdefender for support.

To remove password protection, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **General Settings** tab.
3. Turn off password protection by clicking the switch. Enter the password and then click **OK**.

Note

To modify the password for your product, click the **Change password** link.

4.7. Anonymous usage reports

By default, Bitdefender sends reports containing information about how you use it to Bitdefender servers. This information is essential for improving the product and can help us offer you a better experience in the future. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

In case you want to stop sending Anonymous usage reports, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **Advanced** tab.
3. Click the switch to turn off Anonymous usage reports.

4.8. Special offers and product notifications

When promotional offers are available, the Bitdefender product is set up to notify you through a pop-up window. This gives you the opportunity to benefit from advantageous prices and keep your devices protected for a longer period of time.

Additionally, product notifications can appear when changes are made by user in the product.

To turn on or off special offers and product notifications, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **General Settings** tab.
3. Turn on or off special offers and product notifications by clicking the corresponding switch.

The special offers and product notifications option is enabled by default.

Note
After disabling special offers and product notifications, Bitdefender will continue to keep you informed about special offers when you use a trial version, when your subscription is due to expire, or when you use an expired product version.

5. BITDEFENDER INTERFACE

Bitdefender Total Security 2016 meets the needs of computer beginners and very technical people alike. Its graphical user interface is designed to suit each and every category of users.

To see the status of the product and perform essential tasks, the Bitdefender system tray icon is available at any time.

The main window gives you access to important product information, the program modules, and lets you perform common tasks. From the main window you can access the Bitdefender modules for detailed configuration and advanced administrative tasks, and manage the product's behavior using Autopilot and Profiles.

If you want to keep a constant eye on essential security information and have quick access to key settings, add the Security Widget to your desktop.

5.1. System tray icon

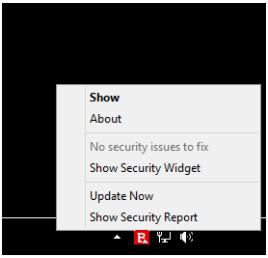
To manage the entire product more quickly, you can use the Bitdefender icon in the system tray.

Note

The Bitdefender icon may not be visible at all times. To make the icon appear permanently, follow these steps:

- In **Windows 7, Windows 8 and Windows 8.1**:
  1. Click the arrow in the lower-right corner of the screen.
  2. Click **Customize...** to open the Notification Area Icons window.
  3. Select the option **Show icons and notifications** for the **Bitdefender Agent** icon.
- In **Windows 10**:
  1. Right-click the taskbar and select **Properties**.
  2. Click **Customize** in the Taskbar window.
  3. Click the **Select which icons appear on the taskbar** link in the **Notifications & actions** window.
  4. Enable the switch next to **Bitdefender Agent**.

If you double-click this icon, Bitdefender will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the Bitdefender product.



Tray Icon

- **Show** - opens the main window of Bitdefender.
- **About** - opens a window where you can see information about Bitdefender and where to look for help in case something unexpected appears.
- **View security issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to *"Fixing issues" (p. 14)*.
- **Hide / Show Security Widget** - enables / disables Security Widget.
- **Update Now** - starts an immediate update. You can follow the update status in the Update panel of the main Bitdefender window.
- **Show Security Report** - opens a window where you can see a weekly status and recommendations for your system. You can follow the recommendations to improve your system security.

The Bitdefender system tray icon informs you when issues affect your computer or how the product operates, by displaying a special symbol, as follows:

Critical issues are affecting the security of your system. They require your immediate attention and must be fixed as soon as possible.
Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
Bitdefender Autopilot is engaged.

If Bitdefender is not working, the system tray icon appears on a gray background: . This usually happens when the license key expires. It can also occur when the Bitdefender services are not responding or when other errors affect the normal operation of Bitdefender.

5.2. Main window

The main Bitdefender window allows you to perform common tasks, quickly fix security issues, view information about product operation and access

the panels from where you configure the product settings. Everything is just a few clicks away.

The window is organized in two main areas:

Upper toolbar
: This is where you can check your computer's security status, configure the Bitdefender behavior in special cases and access important tasks.

Action buttons area
: This is where you can access the Bitdefender Central dashboard account and run different tasks to keep your system protected and running at optimal speed.

The icon in the lower-left corner of the main interface gives you access to the product modules so you can start the configuration of the product settings.

The icon at the top of the main interface lets you manage your account and access the online features of your product from the account dashboard. Here you can also access the Events, the weekly Security Report, and the Help & Support page.

Link	Description
Number of days left	The time remaining before your current subscription expires is displayed. Click the link to open a window where you can see more information about your license key or register your product with a new license key.

5.2.1. Upper toolbar

The upper toolbar contains the following elements:

- **Security Status Area** on the left side of the toolbar, informs you if there are any issues affecting your computer's security and helps you fix them.

  The color of the security status area changes depending on the detected issues and different messages are displayed:

  - **The area is colored green.** There are no issues to fix. Your computer and data are protected.

- **The area is colored yellow.** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
- **The area is colored red.** Critical issues are affecting the security of your system. You should address these issues immediately.

By clicking anywhere inside the security status area, you can access a wizard that will help you easily remove any threats from your computer. For detailed information, please refer to "*Fixing issues*" (p. 14).

- **Autopilot** allows you to engage the Autopilot and enjoy completely silent security. For detailed information, please refer to "*Autopilot*" (p. 17).
- **Profiles** allows you to work, play games or watch movies by saving time configuring the system to postpone maintenance tasks. For detailed information, please refer to "*Profiles*" (p. 168).

5.2.2. Action buttons

Using action buttons you can quickly access your Bitdefender Central account and launch important tasks.

The action buttons available in this area are:

- **Go to Bitdefender Central**. Access your Bitdefender Central account to verify your subscriptions and perform security tasks on the devices you manage.
- **Quick Scan**. Run a quick scan to make sure your computer is clean of viruses.
- **Vulnerability Scan**. Scan your computer for vulnerabilities to make sure that all installed applications, along with the Operating System, are updated and properly functioning.
- **Safepay**. Open Bitdefender Safepay™ to protect your sensitive data while proceeding online transactions.
- **Startup Optimizer**. Decrease your system boot time by excluding unnecessary applications from running at startup.
- **OneClick Optimizer**. Free disk space, fix registry errors and protect your privacy by deleting files that may no longer be useful with a single click on a button.
- **Update**. Update your Bitdefender to make sure that you have the latest malware signatures.

5.3. The Bitdefender modules

The Bitdefender product comes with a number of useful modules to help you stay protected while you work, surf the web or want to make online payments, improve the speed of your system and many others.

Whenever you want to access the modules or to start configuring your product, click the icon in the lower-left corner of the Bitdefender interface.

The modules are separated into three tabs, based on the features they offer:

- Protection
- Privacy
- Tools

5.3.1. Protection

In this tab you can configure your security level, manage friends and spammers, view and edit the network connection settings, and set up what system vulnerabilities to be fixed.

The modules you can manage in the Protection panel are:

Antivirus

Antivirus protection is the foundation of your security. Bitdefender protects you in real-time and on-demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

From the Antivirus module you can easily access the following scan tasks:

- Quick Scan
- System Scan
- Manage Scans
- Rescue Mode

For more information about scan tasks and how to configure antivirus protection, please refer to "*Antivirus protection*" (p. 83).

Web Protection

Web Protection helps you to stay protected against phishing attacks, fraud attempts and private data leaks, while surfing on the Internet.

For more information about how to configure Bitdefender to protect your web activity, please refer to "*Web Protection*" (p. 115).

Vulnerability

The Vulnerability module helps you to keep up to date the operating system and the applications you regularly use.

Click **Vulnerability Scan** under the Vulnerability module to start identifying critical Windows updates, applications updates and weak passwords belonging to Windows accounts.

For more information on configuring vulnerability protection, please refer to "*Vulnerability*" (p. 123).

Firewall

The firewall protects you while you are connected to networks and the Internet by filtering all connection attempts.

For more information about firewall configuration, please refer to "*Firewall*" (p. 127).

Intrusion Detection

Intrusion Detection analyzes system and network activities for unusual behavior and possible attacks.

For more information about how to configure Intrusion Detection to protect your system and network activity, please refer to "*Intrusion Detection*" (p. 135).

Antispam

The Bitdefender antispam module ensures your Inbox stays free of unwanted e-mails by filtering POP3 mail traffic.

For more information about the antispam protection, please refer to "*Antispam*" (p. 106).

Ransomware Protection

The Ransomware Protection module ensures that your personal files stay protected from attacks of online Black Hands.

For more information about how to configure Ransomware Protection to protect your system from ransomware attacks, please refer to "*Ransomware Protection*" (p. 136).

5.3.2. Privacy

In the Privacy tab you can encrypt your private data, protect your online transactions, keep secure your browsing experience, and protect your children by viewing and restricting their online activity.

The modules you can manage in the Privacy panel are:

Data protection

The Data protection module lets you delete files permanently.
Click **File Shredder** under the Data Protection module to start a wizard that will allow you to completely eliminate files from your system.

For more information on configuring Data protection, please refer to "*Data protection*" (p. 117).

Password Manager

Bitdefender Password Manager helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

From the Password Manager module you can select the following tasks:

- **Open Wallet** - opens the existing Wallet database.
- **Lock Wallet** - locks the existing Wallet database.
- **Export Wallet** - allows you to save the existing database to a location on your system.
- **Create new Wallet** - starts a wizard that will allow you to create a new Wallet database.

For more information about configuring Password Manager, please refer to "*Password Manager protection for your credentials*" (p. 144).

Safepay

The Bitdefender Safepay™ browser helps you to keep your online banking, e-shopping and any other type of online transaction private and secure.

Click the **Safepay** action button from the Bitdefender interface to start making online transactions in a secure environment.

For more information about Bitdefender Safepay™, please refer to "*Safepay security for online transactions*" (p. 139).

Parental Advisor

Bitdefender Parental Advisor allows you to monitor what your child is doing on the computer. In case of inappropriate content you can decide to restrict his access to the Internet or to specific applications.

Click **Configure** under the Parental Advisor module to start configuring your children's Windows accounts and monitor their activity wherever you are.

For more information about configuring Parental Advisor, please refer to "*Parental Advisor*" (p. 152).

File Encryption
Create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents.

For more information about how to create encrypted, password-protected logical drives (or vaults) on your computer, please refer to "*File encryption*" (p. 118).

5.3.3. Tools

In the Tools tab you can configure your working profile, improve the system's speed, and manage your devices.

The modules you can manage in the Tools tab are:

Tune-Up
Bitdefender Total Security 2016 offers not just security, it also helps you keep your computer's performance in shape.

In the Tune-Up module you can access a number of useful tools:
- OneClick Optimizer
- Startup Optimizer

For more information about the performance optimization tools, please refer to "*Tune-Up*" (p. 165).

Profiles
Bitdefender Profiles helps you to have a simplified user experience while working, watching a movie or playing a game, by monitoring the product and system working tools. Click **Activate Now** on the upper toolbar in the Bitdefender interface to start using this feature.

Bitdefender lets you to configure the following profiles:
- Work Profile
- Movie Profile
- Game Profile

For more information about how you can configure the profiles module, please refer to "*Profiles*" (p. 168).

Anti-Theft

Bitdefender Anti-Theft protects your computer and data against theft or loss. In case of such an event, this allows you to remotely locate or lock your computer. You can also wipe all data present into your system.

Bitdefender Anti-Theft offers the following features:

- Remote Locate
- Remote Lock
- Remote Wipe
- Remote Alert

For more information about how you can keep your system away from wrong hands, please refer to "*Device Anti-Theft*" (p. 161).

5.4. Security Widget

Security Widget is the quick and easy way to monitor and control Bitdefender Total Security 2016. Adding this small and unintrusive widget to your desktop lets you see critical information and perform key tasks at all times:

- open the main window of Bitdefender.
- monitor scanning activity in real-time.
- monitor the security status of your system and fix any existing issues.
- view when an update is in progress.
- view notifications and get access to the latest events reported by Bitdefender.
- scan files or folders by dragging and dropping one or multiple items over the widget.

Security Widget

The overall security status of your computer is displayed **at the center** of the widget. The status is indicated by the color and shape of the icon that is displayed in this area.

Critical issues are affecting the security of your system.

They require your immediate attention and must be fixed as soon as possible. Click the status icon to begin fixing the reported issues.

Non-critical issues are affecting the security of your system. You should check and fix them when you have the time. Click the status icon to begin fixing the reported issues.

Your system is protected.

When an on-demand scan task is in progress, this animated icon is displayed.

When issues are reported, click the status icon to launch the Fix Issues wizard.

The lower side of the widget displays the unread events counter (the number of outstanding events reported by Bitdefender, if any). Click the event counter, for example for one unread event, to open the Events window. For more information, please refer to "*Events*" (p. 16).

5.4.1. Scanning files and folders

You can use the Security Widget to quickly scan files and folders. Drag any file or folder you want to be scanned and drop it over the **Security Widget**.

The Antivirus Scan wizard will appear and guide you through the scanning process. The scanning options are pre-configured for the best detection results and can not be changed If infected files are detected, Bitdefender will try to disinfect them (remove the malware code). If disinfection fails, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files.

5.4.2. Hide / show Security Widget

When you no longer want to see the widget, click .

To restore Security Widget, use one of the following methods:

- From system tray:
  1. Right-click the Bitdefender icon in the system tray icon.

2. Click **Show Security Widget** in the contextual menu that appears.

- From the Bitdefender interface:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **General Settings** tab.
3. Turn on **Display Security Widget** by clicking the corresponding switch.

5.5. Security Report

The Security Report provides a weekly status for your product and various tips to improve the system protection. These tips are important for managing the overall protection and you can easily see the actions you can take on your system.

The report is generated once a week and it summarizes the relevant information on your product activity so you can easily understand what occurred during this period of time.

The information offered by the Security Report is divided into three categories:

- **Protection** area - view information related to your system protection.
  - **Files Scanned**

    Allows you to see the files scanned by Bitdefender for the week. You can view details, such as the number of scanned files and the number of files cleaned by Bitdefender.

    For more information on the Antivirus protection, please refer to "*Antivirus protection*" (p. 83).
  - **Websites Scanned**

    Allows you to check the number of web pages scanned and blocked by Bitdefender. To protect you from disclosing personal information while browsing, Bitdefender secures your web traffic.

    For more information on Web Protection, please refer to "*Web Protection*" (p. 115).
  - **Vulnerabilities**

    Allows you to easily identify and fix system vulnerabilities in order to make your computer more secure against malware and hackers.

For more information on the Vulnerability scan, please refer to "*Vulnerability*" (p. 123).

- **Events Timeline**

  Allows you to have an overall image of all scanning processes and issues fixed by Bitdefender throughout the week. The events are separated by days.

  For more information on a detailed log of events concerning the activity on your computer, see Events.

- **Privacy** area - view information related to your system privacy.
  - **Files in Vault**

    Allows you to view how many files are secured against unwanted access.

    To find more information about how to create encrypted, password-protected logical drives (or vaults) on your computer, please refer to "*File encryption*" (p. 118).

- **Optimization** area - view information related to the space cleared, optimized applications and how much computer battery you had saved using Battery Mode.
  - **Space cleaned**

    Allows you to view how much space has been cleared during the system optimization process. Bitdefender uses Tune-Up to help improve your system speed.

    For more information on Tune-Up, please refer to "*Tune-Up*" (p. 165).

  - **Battery saved**

    Allows you to see how much battery you have saved while the system ran in Battery Mode.

    For more information on Battery Mode, please refer to "*Battery Mode*" (p. 20).

  - **Apps optimized**

    Allows you to see the number of the applications you have used under the Profiles.

    For more information on Profiles, please refer to "*Profiles*" (p. 168).

5.5.1. Checking the Security Report

The Security Report uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. Using the report, you can configure specific Bitdefender components or take preventive actions to protect your computer and your private data.

To check the Security Report, follow these steps:

1. Access the report:
   - Click the icon at the top of the Bitdefender interface and then select **Security Report** from the drop-down menu.
   - Right-click the Bitdefender icon in the system tray and select **Show Security Report**.
   - Once a report is complete you will receive a pop-up notification. Click **Show** to access the security report.

     A web page will open on your web browser where you can view the generated report.
2. Take a look at the top of the window to see the overall security status.
3. Check our recommendations at the bottom of the page.

The color of the security status area changes depending on the detected issues and different messages are displayed:

- **The area is colored green.** There are no issues to fix. Your computer and data are protected.
- **The area is colored yellow.** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
- **The area is colored red.** Critical issues are affecting the security of your system. You should address these issues immediately.

5.5.2. Turning on or off the Security Report notification

To turn on or off the Security Report notification, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.

2. In the **General Settings** window, select the **General Settings** tab.
3. Click the corresponding switch to turn on or off the Security Report notification.

   The Security Report notification is enabled by default.

6. BITDEFENDER CENTRAL

Bitdefender Central is the web platform where you have access to the product's online features and services and can remotely perform important tasks on devices Bitdefender is installed on. You can log in to your Bitdefender Central account from any computer or mobile device connected to the Internet by going to https://central.bitdefender.com. Once you have access to it, you can start doing the following:

- Download and install Bitdefender on Windows, OS X and Android operating systems. The products available for download are:
  - Bitdefender Total Security 2016
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security
- Manage and renew your Bitdefender subscriptions.
- Add new devices to your network and manage them wherever you are.
- Protect the network devices and their data against theft or loss with Anti-Theft.

6.1. Accessing your Bitdefender Central account

There are several ways to access your Bitdefender Central account. Depending on the task you want to perform, you can use any of the following possibilities:

- From the Bitdefender main interface:
  1. Click the **Go to Bitdefender Central** link in the left part of the Bitdefender interface.
- From Account Info:
  1. Click the icon at the top of the Bitdefender interface, then select **Account Info** from the drop-down menu.
  2. Click the **Go to Bitdefender Central** link in the lower part of the window that appears.
- From your web browser:
  1. Open a web browser on any device with Internet access.

2. Go to: https://central.bitdefender.com.
3. Log in to your account using your e-mail address and password.

6.2. My Subscriptions

The Bitdefender Central platform gives you the possibility to easily manage the subscriptions you have for all your devices.

6.2.1. Check available subscriptions

To check your available subscriptions:

1. Access your Bitdefender Central account.
2. Select the **My Subscriptions** panel.

Here you have information about the availability of the subscriptions you own and the number of devices using each of them.

You can add a new device to a subscription or renew it by selecting a subscription card.

Note
You can have one or more subscriptions on your account provided that the subscriptions are for different products.

6.2.2. Add a new device

If your subscription covers more that one device, you can add a new device and install your Bitdefender Total Security 2016 on it, as follows:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. In the **My Devices** window, click **INSTALL Bitdefender**.
4. Choose **Windows**, then choose one of the two available options:
   - I want to install Bitdefender **On this device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list, then click **Download** to continue.
   - I want to install Bitdefender **On another device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.

5. Wait for the download to complete, then run the installer.

6.2.3. Renew subscription

If you did not opt out for automatically renewing your Bitdefender subscription, you can manually renew it by following these steps:

1. Access your Bitdefender Central account.
2. Select the **My Subscriptions** panel.
3. Select the desired subscription card.
4. Click **Renew** to continue.

A web page opens in your web browser where you can renew your Bitdefender subscription.

6.2.4. Activate subscription

A subscription can be activated during the installation process by using your Bitdefender Central account. Together with the activation process, its validity starts to count-down.

If you have purchased an activation code from one of our resellers or you received it as a present, then you can add its availability to your Bitdefender subscription, provided that they are for the same product.

To activate a subscription using an activation code, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Subscriptions** panel.
3. Click the **ACTIVATION CODE** button, then type the code in the corresponding field.
4. Click **SUBMIT**.

The subscription is now activated. Go to **My Devices** panel, and select **INSTALL Bitdefender** to install the product on one of your devices.

6.3. My Devices

The **My Devices** area in your Bitdefender Central account gives you the possibility to install, manage and take remote actions on your Bitdefender product on any device, provided that it is turned on and connected to the

Internet. The device cards display the device name, protection status and remaining availability on your subscription.

To easily identify your devices, you can customize the device name:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. Click the icon on the desired device card, then select **Settings**.
4. Change the device name in the corresponding field, then select **Save**.

In case the Autopilot is turned off, you can enable it by clicking the switch. Click **Save** to apply the settings.

You can create and assign an owner to each of your devices for better management:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. Click the icon on the desired device card, then select **Profile**.
4. Click **Add owner**, then fill in the corresponding fields, set the Gender, Date of birth and even add a Profile picture.
5. Click **ADD** to save the profile.
6. Select the desired owner from the **Device owner** list, then click **ASSIGN**.

To remotely update Bitdefender on a device, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. Click the icon on the desired device card, then select **Update**.

For more remote actions and information regarding your Bitdefender product on a specific device, click the desired device card.

Once you click on a device card, the following tabs are available:

- **Dashboard**. In this window you can check the protection status of your Bitdefender products and number of remaining days on your subscription. The protection status can be green, when there is no issue affecting your product, or red when the device is at risk. When there are issues affecting

your product, click **View issues** to find out more details. From here you can manually fix issues that are affecting the security of your devices.

- **Protection**. From this window you can remotely run a Quick or a System Scan on your devices. Click the **SCAN** button to start the process. You can also check when the last scan was performed on the device and a report of the latest scan with the most important information is available. For more information about these two scan processes, please refer to "*Running a System Scan*" (p. 90) and to "*Running a Quick Scan*" (p. 90).
- **Optimizer**. Here you can remotely improve a device's performance by rapidly scanning, detecting and cleaning useless files. Click the **START** button, and then select the areas you want to optimize. Click again the **START** button to begin the optimization process. For more details about this feature, please refer to "*Optimizing your system speed with a single click*" (p. 165).
- **Anti-Theft**. In case of misplaced, theft or loss, with the Anti-Theft feature you can locate your device and take remote actions. Click **LOCATE** to find out the position of the device. The last known position will be displayed, along with the time and date. For more details about this feature, please refer to "*Device Anti-Theft*" (p. 161).
- **Vulnerability**. To check a device for vulnerabilities as missing Windows updates, outdated applications, or weak passwords click the **SCAN** button in the Vulnerability tab. Vulnerabilities cannot be fixed remotely. In case any is found, you need to run a new vulnerability scan on the issue device, and then take the recommended actions. For more details about this feature, please refer to "*Vulnerability*" (p. 123).

7. KEEPING BITDEFENDER UP-TO-DATE

New malware is found and identified every day. This is why it is very important to keep Bitdefender up to date with the latest malware signatures.

If you are connected to the Internet through broadband or DSL, Bitdefender takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that. If an update is detected, it is automatically downloaded and installed on your computer.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

Important
To be protected against the latest threats keep Automatic Update turned on.

In some particular situations, your intervention is required in order to keep your Bitdefender protection up-to-date:

- If your computer connects to the Internet through a proxy server, you must configure the proxy settings as described in "*How do I configure Bitdefender to use a proxy Internet connection?*" (p. 77).
- If you do not have Internet connection, you can update Bitdefender manually as described in "*My computer is not connected to the Internet. How do I update Bitdefender?*" (p. 185). The manual update file is released once a week.
- Errors may occur while downloading updates on a slow Internet connection. To find out how to overcome such errors, please refer to "*How to update Bitdefender on a slow Internet connection*" (p. 184).
- If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Bitdefender by user request. For more information, please refer to "*Performing an update*" (p. 44).

7.1. Checking if Bitdefender is up-to-date

To check the time of the last update of your Bitdefender, look on the **Security Status Area**, on the left side of the toolbar.

For detailed information about the latest updates, check the update events:

1. In the main window, click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.
2. In the **Events** window, select **Update** from the corresponding drop-down menu.

You can find out when updates were initiated and information about them (whether they were successful or not, if they require a restart to complete the installation). If required, restart the system at your earliest convenience.

7.2. Performing an update

In order to perform updates, an Internet connection is required.

To start an update, do any of the following:

- Open the Bitdefender interface and click the **Update** action button.
- Right-click the Bitdefender B icon in the system tray and select **Update now**.

The Update module will connect to the Bitdefender update server and it will check for updates. If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings.

> **Important**
> It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

You can also perform updates remotely on your devices, provided that they are turned on and connected to the internet.

To remotely update Bitdefender on a device, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. Click the ⋮ icon on the desired device card, then select **Update**.

7.3. Turning on or off automatic update

To turn on or off automatic update, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **Update** tab.
3. Click the switch to turn on or off the automatic update.
4. A warning window appears. You must confirm your choice by selecting from the menu how long you want the automatic update to be disabled. You can disable the automatic update for 5, 15 or 30 minutes, for an hour, permanently or until a system restart.

Warning
This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If Bitdefender is not updated regularly, it will not be able to protect you against the latest threats.

7.4. Adjusting update settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, Bitdefender will check for updates every hour, over the Internet, and install the available updates without alerting you.

The default update settings are suited for most users and you do not normally need to change them.

To adjust the update settings, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **Update** tab and adjust the settings according to your preferences.

Update frequency

Bitdefender is configured to check for updates every hour. To change the update frequency, drag the slider along the scale to set the desired period of time when the update should occur.

Update location

Bitdefender is configured to update from the Bitdefender update servers on the Internet. The update location is a generic Internet address that is automatically redirected to the closest Bitdefender update server in your region.

Do not change the update location unless advised by a Bitdefender representative or by your network administrator (if you are connected to an office network).

You can switch back to the generic Internet update location by clicking **Default**.

Update processing rules

You can choose between three ways to download and install updates:

- **Silent update** - Bitdefender automatically downloads and implements the update.
- **Prompt before downloading** - every time an update is available, you will be prompted before downloading it.
- **Prompt before installing** - every time an update was downloaded, you will be prompted before installing it.

Some updates require a restart to complete the installation. By default, if an update requires a restart, Bitdefender will keep working with the old files until the user voluntarily restarts the computer. This is to prevent the Bitdefender update process from interfering with the user's work.

If you want to be prompted when an update requires a restart, turn off the **Postpone reboot** option by clicking the corresponding switch.

HOW TO

8. INSTALLATION

8.1. How do I install Bitdefender on a second computer?

If the subscription you have purchased covers more than one computer, you can use your Bitdefender Central account credentials to register a second PC.

To install Bitdefender on a second computer, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. In the **My Devices** window, click **INSTALL Bitdefender**.
4. Choose **Windows**, then choose one of the two available options:
   - I want to install Bitdefender **On this device**.

     From the **Product to be installed** list select Bitdefender Total Security 2016, then click **Download** to continue.
   - I want to install Bitdefender **On another device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.
5. Run the Bitdefender product you have downloaded. Wait until the installation process is completed and close the window.

The new device on which you have installed the Bitdefender product will apear in the Bitdefender Central dashboard.

8.2. When should I reinstall Bitdefender?

In some situations, you may need to reinstall your Bitdefender product.

Typical situations when you would need to reinstall Bitdefender include the following:

- you have reinstalled the operating system.
- you have purchased a new computer.
- you want to change the display language of the Bitdefender interface.

To reinstall Bitdefender you can use the installation disc you purchased or download a new version from your Bitdefender Central account.

For more information about the Bitdefender installation process, please refer to "*Installing your Bitdefender product*" (p. 5).

8.3. Where can I download my Bitdefender product from?

You can install Bitdefender from the installation disc, or using the web installer you can download on your computer from the Bitdefender Central platform.

> **Note**
> Before running the kit, it is recommended to remove any antivirus solution installed on your system. When you use more than one security solution on the same computer, the system becomes unstable.

To install Bitdefender from the Bitdefender Central account, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. In the **My Devices** window, click **INSTALL Bitdefender**.
4. Choose **Windows**, then choose one of the two available options:
   - I want to install Bitdefender **On this device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list, then click **Download** to continue.
   - I want to install Bitdefender **On another device**.

     Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.
5. Run the Bitdefender product you have downloaded.

8.4. How do I use my Bitdefender subscription after a Windows upgrade?

This situation appears when you upgrade your operating system and you want to continue using your Bitdefender subscription.

If you are using a previous Bitdefender version you can upgrade, free of charge, to the latest Bitdefender, as follows:

- From a previous Bitdefender Antivirus version to the latest Bitdefender Antivirus available.
- From a previous Bitdefender Internet Security version to the latest Bitdefender Internet Security available.
- From a previous Bitdefender Total Security version to the latest Bitdefender Total Security available.

There are two cases which may appear:

- You have upgraded the operating system using the Windows Update and you notice Bitdefender is no longer working.

  In this case, you need to reinstall the product using the latest available version.

  To solve this situation, follow these steps:

  1. Remove Bitdefender by following these steps:
     - In **Windows 7**:
       a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
       b. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       c. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       d. Click **Next** to continue.
       e. Wait for the uninstall process to complete, then reboot your system.
     - In **Windows 8 and Windows 8.1**:
       a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
       b. Click **Uninstall a program** or **Programs and Features**.
       c. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       d. Click **Remove** in the window that appears, and then select **I want to reinstall it**.

e. Click **Next** to continue.

f. Wait for the uninstall process to complete, then reboot your system.

- In **Windows 10**:

a. Click **Start**, then click Settings.

b. Click the **System** icon in the Settings area, then select **Installed apps**.

c. Find **Bitdefender Total Security 2016** and select **Uninstall**.

d. Click **Uninstall** again to confirm your choice.

e. Click **Remove** and then select **I want to reinstall it**.

f. Click **Next** to continue.

g. Wait for the uninstall process to complete, then reboot your system.

2. Download the installation file:

a. Access your Bitdefender Central account.

b. Select the **My Devices** panel.

c. In the **My Devices** window, click **INSTALL Bitdefender**.

d. Choose **Windows**, then choose one of the two available options:

- I want to install Bitdefender **On this device**.

  Select Bitdefender Total Security 2016 from the **Product to be installed** list, then click **Download** to continue.

- I want to install Bitdefender **On another device**.

  Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.

3. Locate and double click the installer to start the installation process.

- You changed your system and you want to continue using the Bitdefender protection.

  Therefore, you need to reinstall the product using the latest version.

  To solve this situation:

1. Download the installation file:

a. Access your Bitdefender Central account.

b. Select the **My Devices** panel.

c. In the **My Devices** window, click **INSTALL Bitdefender**.

d. Choose **Windows**, then choose one of the two available options:

- I want to install Bitdefender **On this device**.

  Select Bitdefender Total Security 2016 from the **Product to be installed** list, then click **Download** to continue.

- I want to install Bitdefender **On another device**.

  Select Bitdefender Total Security 2016 from the **Product to be installed** list. Type an e-mail address in the corresponding field, then click **SEND**.

2. Locate and double click the installer to start the installation process.

For more information about the Bitdefender installation process, please refer to "*Installing your Bitdefender product*" (p. 5).

8.5. How do I repair Bitdefender?

If you want to repair your Bitdefender Total Security 2016 from the Windows start menu, follow these steps:

- In **Windows 7**:

  1. Click **Start** and go to **All Programs**.
  2. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  3. Click **Repair** in the window that appears.

     This will take several minutes.
  4. You will need to restart the computer to complete the process.

- In **Windows 8 and Windows 8.1**:

  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  4. Click **Repair** in the window that appears.

     This will take several minutes.

5. You will need to restart the computer to complete the process.

- In **Windows 10**:
  1. Click **Start**, then click Settings.
  2. Click the **System** icon in the Settings area, then select **Apps & features**.
  3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  4. Click **Uninstall** again to confirm your choice.
  5. Click **Repair**.

     This will take several minutes.
  6. You will need to restart the computer to complete the process.

9. SUBSCRIPTIONS

9.1. What Bitdefender product am I using?

To find out which Bitdefender program you have installed:

1. Open the Bitdefender interface.
2. At the top of the window you should see one of the following:
   - Bitdefender Antivirus Plus 2016
   - Bitdefender Internet Security 2016
   - Bitdefender Total Security 2016

9.2. How do I activate Bitdefender subscription using a license key?

If you have a valid license key and want to use it to activate a subscription for Bitdefender Total Security 2016, there are two possible cases:

- You have upgraded from a previous Bitdefender version to the new one:
  1. Once the upgrade to Bitdefender Total Security 2016 is complete, you are asked to log in into your Bitdefender Central account.
  2. Type your login credentials, and click **SIGN IN**
  3. A notification informing you that a subscription was created appears on your account screen. The created subscription will be valid for the remaining days on your license key and for the same number of users.

     Devices that are using previous Bitdefender versions and are registered with the license key you have converted to a subscription need to register the product with the same Bitdefender Central account.
- Bitdefender was not previously installed on the system:
  1. As soon as the installation process is complete, you are asked to log in into your Bitdefender Central account.
  2. Type your login credentials, and click **SIGN IN**
  3. Select the **My Subscriptions** panel.
  4. Click the **Add License Key** button, and type your license key.

5. A subscription with the same availability and number of users of your license key is associated to your account.

10. BITDEFENDER CENTRAL

10.1. How do I log in to Bitdefender Central using another online account?

You have created a new Bitdefender Central account and you want to use it from now on.

To successfully use another account, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Account Info** from the drop-down menu.
2. Click the **Switch Account** button to change the account linked to the computer.
3. Type the e-mail address and the password of your account in the corresponding fields, then click **SIGN IN**.

Note
The Bitdefender product from your device automatically changes according to the subscription associated to the new Bitdefender Central account.
If there is no available subscription associated to the new Bitdefender Central account, or you wish to transfer it from the previous account, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

10.2. How do I reset the password for Bitdefender Central account?

To set a new password for your Bitdefender Central account, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Account Info** from the drop-down menu.
2. Click the **Switch Account** button to change the account linked to the computer.

   A new window appears.
3. Click the **Password reset** link.

4. Type the e-mail address used to create your Bitdefender Central account, then click the **RESET PASSWORD** button.
5. Check your e-mail and click the provided link.
6. Type your Email address in the corresponding field.
7. Type the new password. The password must be at least 8 characters long and include numbers.
8. Click **SET PASSWORD**.

To access your Bitdefender Central account from now on, type your e-mail address and the new password you have just set.

11. SCANNING WITH BITDEFENDER

11.1. How do I scan a file or a folder?

The easiest way to scan a file or folder is to right-click the object you want to scan, point to Bitdefender and select **Scan with Bitdefender** from the menu.

To complete the scan, follow the Antivirus Scan wizard. Bitdefender will automatically take the recommended actions on detected files.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

Typical situations when you would use this scanning method include the following:

- You suspect a specific file or folder to be infected.
- Whenever you download from the Internet files that you think they might be dangerous.
- Scan a network share before copying files to your computer.

11.2. How do I scan my system?

To perform a complete scan on the system, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **System Scan**.
4. Follow the System Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files.

   If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, please refer to "*Antivirus Scan Wizard*" (p. 94).

11.3. How do I schedule a scan?

You can set your Bitdefender product to start scanning important system locations when you are not in the front of the computer.

To schedule a scan, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Manage Scans**.
4. Choose the scan type that you want to schedule, System Scan or Quick Scan, then click **Scan Options**.

   Alternatively, you can create a scan type to suit your needs by clicking **New custom task**.
5. Enable the **Schedule** switch.

   Select one of the corresponding options to set a schedule:

   - At system startup
   - Once
   - Periodically

In the **Scan targets** window you can select the locations you want to be scanned.

11.4. How do I create a custom scan task?

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a customized scan task.

To create a customized scan task, proceed as follows:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Manage Scans**.
4. Click **New custom task**. In the **Basic** tab enter a name for the scan and select the locations to be scanned.
5. If you want to configure the scanning options in detail, select the **Advanced** tab.

   You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level.

You can also choose to shutdown the computer when the scan is over if no threats are found. Remember that this will be the default behavior every time you run this task.

6. Click **OK** to save the changes and close the window.
7. Use the corresponding switch if you want to set a schedule for your scan task.
8. Click **Start Scan** and follow the scan wizard to complete the scan. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
9. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

11.5. How do I exclude a folder from being scanned?

Bitdefender allows excluding specific files, folders or file extensions from scanning.

Exclusions are to be used by users having advanced computer knowledge and only in the following situations:

- You have a large folder on your system where you keep movies and music.
- You have a large archive on your system where you keep different data.
- You keep a folder where you install different types of software and applications for testing purposes. Scanning the folder may result in losing some of the data.

To add the folder to the Exclusions list, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Exclusions** tab.
4. Make sure **Exclusions for files** is turned on by clicking the switch.
5. Click the **Excluded files and folders** link.
6. Click the **Add** button, located at the top of the exclusions table.
7. Click **Browse**, select the folder that you want to be excluded from scanning and then click **OK**.

8. Click **Add** and then **OK** to save the changes and close the window.

11.6. What to do when Bitdefender detected a clean file as infected?

There may be cases when Bitdefender mistakenly flags a legitimate file as being a threat (a false positive). To correct this error, add the file to the Bitdefender Exclusions area:

1. Turn off the Bitdefender real-time antivirus protection:
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Protection** tab.
   c. Click the **Antivirus** module.
   d. In the **Antivirus** window, select the **Shield** tab.
   e. Click the switch to turn off **On-access scanning**.

      A warning window appears. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until a system restart.
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 79).
3. Restore the file from the Quarantine area:
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Protection** tab.
   c. Click the **Antivirus** module, then select the **Quarantine** tab.
   d. Select the file and click **Restore**.
4. Add the file to the Exclusions list. To find out how to do this, please refer to "*How do I exclude a folder from being scanned?*" (p. 60).
5. Turn on the Bitdefender real-time antivirus protection.
6. Contact our support representatives so that we may remove the detection signature. To find out how to do this, please refer to "*Asking for help*" (p. 205).

11.7. How do I check what viruses Bitdefender detected?

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues.

The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check a scan log or any detected infection at a later time, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.
2. In the **Events** window, select **Antivirus** from the corresponding drop-down menu.

   This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
3. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
4. To open a scan log, click **View log**.

   If you want to run again the same scan, click the **Rescan** button.

12. PARENTAL ADVISOR

12.1. How do I protect my children from online threats?

Bitdefender Parental Advisor allows you to restrict access to the Internet and to specific applications, preventing your children from viewing inappropriate content whenever you are not around.

To configure the Parental Advisor, follow these steps:

1. Create limited (standard) Windows user accounts for your children to use. For more information, please refer to "*How do I create Windows user accounts?*" (p. 67).
2. Make sure you are logged on to the computer with an administrator account. Only users with administrative rights on the system (system administrators) can access and configure Parental Advisor.
3. Configure Parental Advisor for the Windows user accounts your children use.
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Privacy** tab.
   c. Under the **Parental Advisor** module, select **Configure**.

      You are redirected to the Bitdefender Central web page. Make sure that you are logged in with your credentials.
   d. The Parental Advisor dashboard opens in a new window. This is where you can check and configure the Parental Advisor settings.
   e. Click **ADD PROFILE** on the right-side of the **My Children** window.
   f. Set specific information in the corresponding fields, such as: name, e-mail, gender, and date of birth, and then click **CONTINUE**.

      Based on children development standards, setting the child's date of birth automatically loads specifications considered appropriate for his age category.
   g. If your child's device already has Bitdefender Total Security 2016 installed, select his device from the available list, and then click **CONTINUE**.

If your child's device has no Bitdefender product with the Parental Advisor feature included, click **Add a new device**. Select the operating system of his device, then click **CONTINUE**.

Type the e-mail address where we should send the installation download link of the Bitdefender Parental Advisor application.

On Windows based devices, the Bitdefender Total Security 2016 you have included in your subscription should be downloaded and installed. On Android devices, the Bitdefender Parental Advisor Agent should be downloaded and installed.

Check your children's activities and change the Parental Advisor settings using Bitdefender Central from any computer or mobile device connected to the Internet.

12.2. How do I block my child's access to a website?

Bitdefender Parental Advisor allows you to control the content accessed by your child while using his device and enables you to block access to a website.

To block access to a website, you need to add it to the Exclusions list, as follows:

1. Go to: https://central.bitdefender.com.
2. Log in to your account using your e-mail address and password.
3. Click **Parental Advisor** to access the dashboard.
4. Select your child's profile from the **My Children** window.
5. Select the **Interests** tab.
6. Click the **MANAGE** button.
7. Type the web page you want to block in the corresponding field.
8. Select **Allow** or **Deny**.
9. Click **Done** to save the changes.

12.3. How do I prevent my child from playing a game?

Bitdefender Parental Advisor allows you to control the content accessed by your child while using the computer.

To block access to a game, follow these steps:

1. Go to: https://central.bitdefender.com.
2. Log in to your account using your e-mail address and password.
3. Click **Parental Advisor** to access the dashboard.
4. Select your child's profile from the My Children window.
5. Select the **Activities** tab.

   A list with cards is displayed. The cards represent the apps your child uses.
6. Select the card with the app you want your child to stop using.

   The check mark symbol that appears indicates that your child will not be able to use the app.

12.4. How do I prevent my child from getting in contact with untrusted persons?

Bitdefender Parental Advisor gives you the possibility to block phone calls from unknown phone numbers or from friends from your child's phone list.

To block a specific contact, follow these steps:

1. Go to: https://central.bitdefender.com.

   Make sure that you are logged in with your credentials.
2. Click **Parental Advisor** to access the dashboard.
3. Click the ⋮ icon on the desired profile card, and then select **Edit**.
4. Type in the corresponding field the phone number of your child, then click **SAVE**.
5. Select the profile of the child you want to set restrictions.
6. Select the **Friends** tab.

   A list with cards is displayed. The cards represent the contacts from your child's phone.
7. Select the card with the phone number you want block.

   The check mark symbol that appears indicates that your child will not be reached by the selected phone number.

To block unknown phone numbers, enable the **Block no caller ID interactions** switch.

12.5. How can I set a location as safe or restricted for my child?

Bitdefender Parental Advisor allows you to set a location as safe or restricted for your child.

To set a location, follow these steps:

1. Go to: https://central.bitdefender.com.

   Make sure that you are logged in with your credentials.
2. Click **Parental Advisor** to access the dashboard.
3. Select your child's profile from the **My Children** window.
4. Select the **Places** tab.
5. Click **Devices** in the frame you have in the **Places** window.
6. Click **CHOOSE DEVICES**, and then select the device you want to configure.
7. In the **Areas** window, click the **ADD AREA** button.
8. Choose the type of the location, **Safe** or **Restricted**.
9. Type a valid name for the area where your child has permissions to go or not.
10. In the **Original Location**, type the town where your child should be located, and then choose the district from the list that appears.
11. Set the range that should be applied for monitoring from the **Radius** slide bar.
12. Click **ADD AREA** to save your settings.

Whenever you want to set a restricted location as safe, or a safe location as restricted, click it, and then select the **EDIT AREA** button. Depending on the change you want to make, select the **SAFE** or the **RESTRICTED** option, and then click **UPDATE AREA**.

12.6. How do I create Windows user accounts?

A Windows user account is a unique profile that includes all the settings, privileges and personal files for each user. Windows accounts let the home PC administrator control access for each user.

Setting up user accounts comes in handy when the PC is used by both parents and children – a parent can set up accounts for each child.

Choose which operating system you have to find out how to create Windows accounts.

- **Windows 7:**
  1. Log on to your computer as an administrator.
  2. Click Start, click Control Panel, and then click User Accounts.
  3. Click Create a new account.
  4. Type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.
  5. For the account type, click Standard, and then Create Account. Limited accounts are appropriate for children because they cannot make system-wide changes or install certain applications.
  6. Your new account will have been created and you will see it listed in the Manage Accounts screen.
- **Windows 8 and Windows 8.1:**
  1. Log on to your computer as an administrator.
  2. Point your mouse to the upper right corner of the screen, click Settings and then click Change PC settings.
  3. Click Users in the left side menu and then click Add a user.

     You can create either a Microsoft account or a Local account. Read the description of each account type and follow the on-screen instructions to create a new account.
- **Windows 10**:
  1. Log on to your computer as an administrator.
  2. Click Start, then click Settings.
  3. Select Accounts, then select Family & other.

4. Click Add someone else on this PC.
5. You can create either a Microsoft account or a Local account. Read the description of each account type and follow the on-screen instructions to create a new account.

Note
Now that you have added new user accounts, you can create passwords for the accounts.

12.7. How to remove a child profile

If you want to remove an existent child profile, follow these steps:

1. Go to: https://central.bitdefender.com.
2. Log in to your account using your e-mail address and password.
3. Click **Parental Advisor** to access the dashboard.
4. Click the ⋮ icon from the child's profile you want to delete, and then choose **Remove**.

13. PRIVACY PROTECTION

13.1. How do I make sure my online transaction is secure?

To make sure your online operations remain private, you can use the browser provided by Bitdefender to protect your transactions and home banking applications.

Bitdefender Safepay™ is a secured browser designed to protect your credit card information, account number or any other sensitive data you may enter while accessing different online locations.

To keep your online activity secure and private, follow these steps:

1. Click the **Safepay** action button from the Bitdefender interface.
2. Click the button to access the **Virtual Keyboard**.
3. Use the **Virtual Keyboard** when typing sensitive information such as your passwords.

13.2. What can I do if my device has been stolen?

Mobile device theft, whether it is a smartphone, a tablet or a laptop is one of the main issues today affecting individuals and organizations throughout the world.

Bitdefender Anti-Theft allows you to not only locate and lock the stolen device, but also wipe all data to ensure that it will not be used by the thief.

To access the Anti-Theft features from your account, follow these steps:

1. Access your Bitdefender Central account.
2. Select the **My Devices** panel.
3. In the **My Devices** window, select the issue device.
4. Click **Anti-Theft**.
5. Select the feature you want to use:
   - **LOCATE** - display your device's location on Google Maps.
   - **Wipe** - delete all data from your computer.

Important
After you wipe a device, all Anti-Theft features cease to function.

- **Lock** - lock your computer and set a numeric PIN code for unlocking it.
- **Alert** - send an alert on the device.

13.3. How do I use file vaults?

The Bitdefender File Vault enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. Physically, the vault is a file stored on the local hard drive having the .bvd extension.

When you create a file vault, two aspects are important: the size and the password. The default 100 MB size should be enough for your private documents, Excel files and other similar data. However, for videos or other large files you may need more space.

To securely store your confidential or sensitive files or folders in Bitdefender file vaults, follow these steps:

- **Create a file vault and set a strong password for it.**

  To create a vault, right-click an empty area of the desktop or in a folder on your computer, point to **Bitdefender** > **Bitdefender File Vault** and select **Create File Vault**.

  A new window appears. Proceed as follows:

  1. In the **Start fresh** area, click **Create new**.
  2. Click **Browse**, select the location of the vault and save the vault file under the desired name.
  3. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in **My Computer**.
  4. Type the vault password in the **Password** and **Confirm** fields.
  5. If you want to change the default size (100 MB) of the vault, type the desired value in the **Vault size (MB)** field.
  6. Click the **Create**.

Note
When you open the vault, a virtual disk drive appears in **My Computer**. The drive is labeled with the drive letter assigned to the vault.

- **Add the files or folders you want to keep safe to the vault.**

  In order to add a file to a vault, you must first open the vault.

  1. Browse to the .bvd vault file.
  2. Right-click the vault file, point to Bitdefender File Vault and select **Open**.
  3. In the window that appears, select a drive letter to assign to the vault, enter the password and click **Open**.

  You can now perform operations on the drive that corresponds to the desired file vault using Windows Explorer, just as you would with a regular drive. To add a file to an open vault, you can also right-click the file, point to Bitdefender File Vault and select **Add to file vault**.

- **Keep the vault locked at all times.**

  Only open vaults when you need to access them or manage their content. To lock a vault, right-click the corresponding virtual disk drive from **My Computer**, point to **Bitdefender File Vault** and select **Lock**.

- **Make sure not to delete the .bvd vault file.**

  Deleting the file also deletes the vault contents.

For more information about operating with file vaults, please refer to *"File encryption"* (p. 118).

13.4. How do I remove a file permanently with Bitdefender?

If you want to remove a file permanently from your system, you need to delete the data physically from your hard disk.

The Bitdefender File Shredder will help you to quickly shred files or folders from your computer using the Windows contextual menu, by following these steps:

1. Right-click the file or folder you want to permanently delete, point to Bitdefender and select **File Shredder**.
2. A confirmation window appears. Click **Yes** to start the File Shredder wizard.

3. Wait for Bitdefender to finish shredding the files.
4. The results are displayed. Click **Close** to exit the wizard.

14. TUNE-UP

14.1. How do I improve my system performance?

The system performance depends not only on the hardware configuration, such as the CPU load, memory usage and hard disk space. It is also directly connected to your software configuration and to your data management.

These are the main actions you can take with Bitdefender to improve your system's speed and performance:

- "*Optimize your system performance with a single click*" (p. 73)
- "*Scan your system periodically*" (p. 73)

14.1.1. Optimize your system performance with a single click

The OneClick Optimizer option saves you valuable time when you want a quick way to improve your system performance by rapidly scanning, detecting and cleaning useless files.

To start the OneClick Optimizer process, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Under the **Tune-Up** module, select **OneClick Optimizer**.
4. Let Bitdefender search for files that can be deleted, then click the **Optimize** button to finish the process.

Or quicker, click the **OneClick Optimizer** action button from the Bitdefender interface.

For more information about how you can improve the speed of your computer with a single click, please refer to "*Optimizing your system speed with a single click*" (p. 165).

14.1.2. Scan your system periodically

Your system speed and its general behavior can also be affected by malware.

Make sure to scan your system periodically, at least once a week.

It is recommended to use the System Scan because it scans for all types of malware threatening the security of your system and it also scans inside archives.

To start the System Scan, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **System Scan**.
4. Follow the wizard steps.

14.2. How can I improve my system startup time?

Unnecessary applications that are annoyingly slowing down booting time when you open your PC can be disabled or postponed from opening with the Startup Optimizer thus saving you valuable time.

To use the Startup Optimizer, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Under the **Tune-Up** module, select **Startup Optimizer**.
4. Select the applications that you want to delay at system startup.

Or quicker, click the **Startup Optimizer** action button from the Bitdefender interface.

For more information on how to optimize your PC's booting time, please refer to "*Optimizing your PC's boot time*" (p. 166).

15. USEFUL INFORMATION

15.1. How do I test my antivirus solution?

To make sure that your Bitdefender product is properly running, we recommend you using the Eicar test.

The Eicar test allows you to check your antivirus protection using a safe file developed for this purpose.

To test your antivirus solution, follow these steps:

1. Download the test from the official webpage of the EICAR organization http://www.eicar.org/.
2. Click the **Anti-Malware Testfile** tab.
3. Click **Download** on the left-side menu.
4. From **Download area using the standard protocol http** click the **eicar.com** test file.
5. You will be informed that the page you are trying to access contains the EICAR-Test-File (not a virus).

   If you click **I understand the risks, take me there anyway**, the download of the test will begin and a Bitdefender pop-up will inform you that a virus was detected.

   Click **More details** to find out more information about this action.

If you do not receive any Bitdefender alert, we recommend you to contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

15.2. How do I remove Bitdefender?

If you want to remove your Bitdefender Total Security 2016, follow these steps:

- In **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  3. Select **Remove**, and then select **I want to permanently remove it**.
  4. Click **Next** to continue.

5. Wait for the uninstall process to complete, then reboot your system.

- In **Windows 8 and Windows 8.1**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  4. Select **Remove**, and then select **I want to permanently remove it**.
  5. Click **Next** to continue.
  6. Wait for the uninstall process to complete, then reboot your system.
- In **Windows 10**:
  1. Click **Start**, then click Settings.
  2. Click the **System** icon in the Settings area, then select **Installed apps**.
  3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  4. Click **Uninstall** again to confirm your choice.
  5. Select **Remove**, and then select **I want to permanently remove it**.
  6. Click **Next** to continue.
  7. Wait for the uninstall process to complete, then reboot your system.

15.3. How do I automatically shut down the computer after the scan is over?

Bitdefender offers multiple scan tasks that you can use to make sure your system is not infected with malware. Scanning the entire computer may take longer time to complete depending on your system's hardware and software configuration.

For this reason, Bitdefender allows you to configure Bitdefender to shut down your system as soon as the scan is over.

Consider this example: you have finished your work at the computer and you want to go to sleep. You would like to have your entire system checked for malware by Bitdefender.

This is how you set up Bitdefender to shut down your system at the end of the scan:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Manage Scans**.
4. In the **Manage Scan Tasks** window, click **New custom task** to enter a name for the scan and select the locations to be scanned.
5. If you want to configure the scanning options in detail, select the **Advanced** tab.
6. Choose to shutdown the computer when the scan is over if no threats are found.
7. Click **OK** to save the changes and close the window.
8. Click the **Start Scan** button to scan your system.

If no threats are found, the computer will shut down.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, please refer to "*Antivirus Scan Wizard*" (p. 94).

15.4. How do I configure Bitdefender to use a proxy Internet connection?

If your computer connects to the Internet through a proxy server, you must configure Bitdefender with the proxy settings. Normally, Bitdefender automatically detects and imports the proxy settings from your system.

Important
Home Internet connections do not normally use a proxy server. As a rule of thumb, check and configure the proxy connection settings of your Bitdefender program when updates are not working. If Bitdefender can update, then it is properly configured to connect to the Internet.

To manage the proxy settings, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.

2. In the **General Settings** window, select the **Advanced** tab.
3. Turn on Proxy usage by clicking the switch.
4. Click the **Manage proxies** link.
5. There are two options to set the proxy settings:
   - **Import proxy settings from default browser** - proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.

     Note
     Bitdefender can import proxy settings from the most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.

   - **Custom proxy settings** - proxy settings that you can configure yourself. The following settings must be specified:
     - **Address** - type in the IP of the proxy server.
     - **Port** - type in the port Bitdefender uses to connect to the proxy server.
     - **Username** - type in a user name recognized by the proxy.
     - **Password** - type in the valid password of the previously specified user.
6. Click **OK** to save the changes and close the window.

Bitdefender will use the available proxy settings until it manages to connect to the Internet.

15.5. Am I using a 32 bit or a 64 bit version of Windows?

To find out if you have a 32 bit or a 64 bit operating system, follow these steps:

- In **Windows 7**:
  1. Click **Start**.
  2. Locate **Computer** on the **Start** menu.
  3. Right-click **Computer** and select **Properties**.
  4. Look under **System** in order to check the information about your system.
- In **Windows 8 and Windows 8.1**:

1. From the Windows Start screen, locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then right-click its icon.
2. Select **Properties** in the bottom menu.
3. Look in the System area to see your system type.

- In **Windows 10**:
  1. Type "System" in the search box from the taskbar and click its icon.
  2. Look in the System area to find information about your system type.

15.6. How do I display hidden objects in Windows?

These steps are useful in those cases where you are dealing with a malware situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

1. Click **Start**, go to **Control Panel**.

   In **Windows 8 and Windows 8.1**: From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
2. Select **Folder Options**.
3. Go to **View** tab.
4. Select **Show hidden files and folders**.
5. Clear **Hide extensions for known file types**.
6. Clear **Hide protected operating system files**.
7. Click **Apply**, then click **OK**.

In **Windows 10**:

1. Type "Show hidden files and folders" in the search box from the taskbar and click its icon.
2. Select **Show hidden files, folders, and drives**.
3. Clear **Hide extensions for known file types**.
4. Clear **Hide protected operating system files**.
5. Click **Apply**, then click **OK**.

15.7. How do I remove other security solutions?

The main reason for using a security solution is to provide protection and safety for your data. But what happens when you have more than one security product on the same system?

When you use more than one security solution on the same computer, the system becomes unstable. The Bitdefender Total Security 2016 installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation, follow these steps:

- In **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Wait for the uninstall process to complete, then reboot your system.
- In **Windows 8 and Windows 8.1**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Wait a few moments until the installed software list is displayed.
  4. Find the name of the program you want to remove and select **Uninstall**.
  5. Wait for the uninstall process to complete, then reboot your system.
- In **Windows 10**:
  1. Click **Start**, then click Settings.
  2. Click the **System** icon in the Settings area, then select **Installed apps**.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Click **Uninstall** again to confirm your choice.
  5. Wait for the uninstall process to complete, then reboot your system.

If you fail to remove the other security solution from your system, get the uninstall tool from the vendor website or contact them directly in order to provide you with the uninstall guidelines.

15.8. How do I restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to viruses preventing Windows from starting normally. In Safe Mode only a few applications work and Windows loads just the basic drivers and a minimum of operating system components. This is why most viruses are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

1. Restart the computer.
2. Press the **F8** key several times before Windows starts in order to access the boot menu.
3. Select **Safe Mode** in the boot menu or **Safe Mode with Networking** if you want to have Internet access.
4. Press **Enter** and wait while Windows loads in Safe Mode.
5. This process ends with a confirmation message. Click **OK** to acknowledge.
6. To start Windows normally, simply reboot the system.

MANAGING YOUR SECURITY

16. ANTIVIRUS PROTECTION

Bitdefender protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on). The protection Bitdefender offers is divided into two categories:

- On-access scanning - prevents new malware threats from entering your system. Bitdefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.

  On-access scanning ensures real-time protection against malware, being an essential component of any computer security program.

  Important
  To prevent viruses from infecting your computer keep **on-access scanning** enabled.

- On-demand scanning - allows detecting and removing the malware that already resides in the system. This is the classic scan initiated by the user - you choose what drive, folder or file Bitdefender should scan, and Bitdefender scans it - on-demand.

Bitdefender automatically scans any removable media that is connected to the computer to make sure it can be safely accessed. For more information, please refer to "*Automatic scan of removable media*" (p. 97).

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned. For more information, please refer to "*Configuring scan exclusions*" (p. 99).

When it detects a virus or other malware, Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to contain the infection. For more information, please refer to "*Managing quarantined files*" (p. 102).

If your computer has been infected with malware, please refer to "*Removing malware from your system*" (p. 196). To help you clean your computer of malware that cannot be removed from within the Windows operating system, Bitdefender provides you with Rescue Mode. This is a trusted environment, especially designed for malware removal, which enables you to boot your computer independent of Windows. When the computer runs in Rescue Mode, Windows malware is inactive, making it easy to remove.

To protect you against unknown malicious applications, Bitdefender uses Active Threat Control, an advanced heuristic technology, which continuously monitors the applications running on your system. Active Threat Control automatically blocks applications that exhibit malware-like behavior to stop them from damaging your computer. Occasionally, legitimate applications may be blocked. In such situations, you can configure Active Threat Control not to block those applications again by creating exclusion rules. To learn more, please refer to "*Active Threat Control*" (p. 103).

16.1. On-access scanning (real-time protection)

Bitdefender provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files and e-mail messages.

The default real-time protection settings ensure good protection against malware, with minor impact on system performance. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels. Or, if you are an advanced user, you can configure the scan settings in detail by creating a custom protection level.

16.1.1. Turning on or off real-time protection

To turn on or off real-time protection against malware, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Shield** tab.
4. Click the switch to turn on or off On-access scanning.
5. If you want to disable real-time protection, a warning window appears. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until a system restart. The real-time protection will automatically turn on when the selected time will expire.

Warning

This is a critical security issue. We recommend you to disable real-time protection for as little time as possible. If real-time protection is disabled, you will not be protected against malware threats.

16.1.2. Adjusting the real-time protection level

The real-time protection level defines the scan settings for real-time protection. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels.

To adjust the real-time protection level, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Shield** tab.
4. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

16.1.3. Configuring the real time protection settings

Advanced users might want to take advantage of the scan settings Bitdefender offers. You can configure the real-time protection settings in detail by creating a custom protection level.

To configure the real time protection settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Shield** tab.
4. Click **Custom**.
5. Configure the scan settings as needed.
6. Click **OK** to save the changes and close the window.

Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan options for accessed files.** You can set Bitdefender to scan all accessed files or applications (program files) only. Scanning all accessed

files provides best protection, while scanning applications only can be used for better system performance.

By default, both local folders and network shares are subject to on-access scanning. For better system performance, you can exclude network locations from on-access scanning.

Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.

  If you decide on using this option, you can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).

- **Scan options for e-mail and HTTP traffic.** To prevent malware from being downloaded to your computer, Bitdefender automatically scans the following malware entry points:
  - incoming and outgoing e-mails
  - HTTP traffic

  Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

Though not recommended, you can disable e-mail or web antivirus scan to increase system performance. If you disable the corresponding scan options, the e-mails and files received or downloaded from the Internet will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the malware when the infected files are accessed (opened, moved, copied or executed).

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan for keyloggers.** Select this option to scan your system for keylogger applications. Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.
- **Scan at system boot.** Select the Early boot scan option to scan your system at startup as soon as all its critical services are loaded. The mission of this feature is to improve virus detection at system startup and the boot time of your system.

Actions taken on detected malware

You can configure the actions taken by the real-time protection.

To configure the actions, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Shield** tab.
4. Click **Custom**.
5. Select the **Actions** tab, and configure the scan settings as needed.
6. Click **OK** to save the changes and close the window.

The following actions can be taken by the real time protection in Bitdefender:

Take proper actions

Bitdefender will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection.

  Files that cannot be disinfected are moved to quarantine in order to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 102).

  Important

  For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

  By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Archives containing infected files.**
  - Archives that contain only infected files are deleted automatically.
  - If an archive contains both infected and clean files, Bitdefender will attempt to delete the infected files provided it can reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

Move files to quarantine
Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 102).

Deny access
In case an infected file is detected, the access to this will be denied.

16.1.4. Restoring the default settings

The default real-time protection settings ensure good protection against malware, with minor impact on system performance.

To restore the default real-time protection settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Shield** tab.
4. Click **Default**.

16.2. On-demand scanning

The main objective for Bitdefender is to keep your computer clean of viruses. This is done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install Bitdefender. This is why it's a very good idea to scan your computer for resident viruses after you've installed Bitdefender. And it's definitely a good idea to frequently scan your computer for viruses.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

16.2.1. Scanning a file or folder for malware

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned, point to

Bitdefender and select **Scan with Bitdefender**. The Antivirus Scan wizard will appear and guide you through the scanning process. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

16.2.2. Running a Quick Scan

Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

To run a Quick Scan, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Quick Scan**.
4. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

Or quicker, click the **Quick Scan** action button from the Bitdefender interface.

16.2.3. Running a System Scan

The System Scan task scans the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others.

> **Note**
> Because **System Scan** performs a thorough scan of the entire system, the scan may take a while. Therefore, it is recommended to run this task when you are not using your computer.

Before running a System Scan, the following are recommended:

- Make sure Bitdefender is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Bitdefender from detecting new malware found since the last update. For more information, please refer to "*Keeping Bitdefender up-to-date*" (p. 43).
- Shut down all open programs.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, please refer to "*Configuring a custom scan*" (p. 91).

To run a System Scan, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **System Scan**.
4. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

16.2.4. Configuring a custom scan

To configure a scan for malware in detail and then run it, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Manage Scans**.
4. Click **New custom task**. In the **Basic** tab enter a name for the scan and select the locations to be scanned.
5. If you want to configure the scanning options in detail, select the **Advanced** tab. A new window appears. Follow these steps:
   a. You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

      Advanced users might want to take advantage of the scan settings Bitdefender offers. To configure the scan options in detail, click **Custom**. You can find information about them at the end of this section.

   b. You can also configure these general options:

      - **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.

- **Minimize Scan Wizard to system tray.** Minimizes the scan window to the system tray. Double-click the Bitdefender icon to open it.
- Specify the action to be taken if no threats are found.

c. Click **OK** to save the changes and close the window.

6. If you want to set a schedule for your scan task, use the **Schedule** switch in the Basic window. Select one of the corresponding options to set a schedule:
   - At system startup
   - Once
   - Periodically
7. Click **Start Scan** and follow the Antivirus Scan wizard to complete the scan. Depending on the locations to be scanned, the scan may take a while. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
8. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan files.** You can set Bitdefender to scan all types of files or applications (program files) only. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa;

ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan options for archives.** Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note
  Scanning archived files increases the overall scanning time and requires more system resources.

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan memory.** Select this option to scan programs running in your system's memory.
- **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
- **Scan cookies.** Select this option to scan the cookies stored by browsers on your computer.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Ignore commercial keyloggers.** Select this option if you have installed and use commercial keylogger software on your computer. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.

- **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.

16.2.5. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder, point to Bitdefender and select **Scan with Bitdefender**), the Bitdefender Antivirus Scan wizard will appear. Follow the wizard to complete the scanning process.

Note

If the scan wizard does not appear, the scan may be configured to run silently, in the background. Look for the scan progress icon in the system tray. You can click this icon to open the scan window and to see the scan progress.

Step 1 - Perform scan

Bitdefender will start scanning the selected objects. You can see real-time information about the scan status and statistics (including the elapsed time, an estimation of the remaining time and the number of detected threats).

Wait for Bitdefender to finish scanning. The scanning process may take a while, depending on the complexity of the scan.

Stopping or pausing the scan. You can stop scanning anytime you want by clicking **Stop**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

Password-protected archives. When a password-protected archive is detected, depending on the scan settings, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. The following options are available:

- **Password.** If you want Bitdefender to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.
- **Don't ask for a password and skip this object from scan.** Select this option to skip scanning this archive.
- **Skip all password-protected items without scanning them.** Select this option if you do not want to be bothered about password-protected

archives. Bitdefender will not be able to scan them, but a record will be kept in the scan log.

Choose the desired option and click **OK** to continue scanning.

Step 2 - Choose actions

At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

Note

When you run a quick scan or a full system scan, Bitdefender will automatically take the recommended actions on detected files during the scan. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

The infected objects are displayed in groups, based on the malware they are infected with. Click the link corresponding to a threat to find out more information about the infected objects.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues. One or several of the following options can appear on the menu:

Take proper actions

Bitdefender will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection.

  Files that cannot be disinfected are moved to quarantine in order to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 102).

Important

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

  By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Archives containing infected files.**
  - Archives that contain only infected files are deleted automatically.
  - If an archive contains both infected and clean files, Bitdefender will attempt to delete the infected files provided it can reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

Delete

Removes detected files from the disk.

If infected files are stored in an archive together with clean files, Bitdefender will attempt to delete the infected files and reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

Take no action

No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

Click **Continue** to apply the specified actions.

Step 3 - Summary

When Bitdefender finishes fixing the issues, the scan results will appear in a new window. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.

Click **Close** to close the window.

Important

In most cases Bitdefender successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. If required, please restart your system in order to complete the cleaning process. For more information and instructions on how to remove malware manually, please refer to "*Removing malware from your system*" (p. 196).

16.2.6. Checking scan logs

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues in the Antivirus window. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check a scan log or any detected infection at a later time, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.
2. In the **Events** window, select **Antivirus** from the corresponding drop-down menu.

   This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
3. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
4. To open the scan log, click **View log**. If you want to run again the same scan, click the **Rescan** button.

16.3. Automatic scan of removable media

Bitdefender automatically detects when you connect a removable storage device to your computer and scans it in the background. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

You can configure automatic scan separately for each category of storage devices. Automatic scan of mapped network drives is off by default.

16.3.1. How does it work?

When it detects a removable storage device, Bitdefender starts scanning it for malware in the background (provided automatic scan is enabled for that type of device). A Bitdefender scan icon will appear in the system tray. You can click this icon to open the scan window and to see the scan progress.

If Autopilot is on, you will not be bothered about the scan. The scan will only be logged and information about it will be available in the Events window.

If Autopilot is off:

1. You will be notified through a pop-up window that a new device has been detected and it is being scanned.
2. In most cases, Bitdefender automatically removes detected malware or isolates infected files into quarantine. If there are unresolved threats after the scan, you will be prompted to choose the actions to be taken on them.

   Note
   Take into account that no action can be taken on infected or suspicious files detected on CDs/DVDs. Similarly, no action can be taken on infected or suspicious files detected on mapped network drives if you do not have the appropriate privileges.

3. When the scan is completed, the scan results window is displayed to inform you if you can safely access files on the removable media.

This information may be useful to you:

- Please be careful when using a malware-infected CD/DVD, because the malware cannot be removed from the disc (the media is read-only). Make sure real-time protection is turned on to prevent malware from spreading to your system. It is best practice to copy any valuable data from the disc to your system and then dispose of the disc.
- In some cases, Bitdefender may not be able to remove malware from specific files due to legal or technical constraints. Such an example are

files archived using a proprietary technology (this is because the archive cannot be recreated correctly).

To find out how to deal with malware, please refer to "*Removing malware from your system*" (p. 196).

16.3.2. Managing removable media scan

To manage automatic scan of removable media, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Exclusions** tab.

For best protection, it is recommended to turn on automatic scan for all types of removable storage devices.

The scanning options are pre-configured for the best detection results. If infected files are detected, Bitdefender will try to disinfect them (remove the malware code) or to move them to quarantine. If both actions fail, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

16.4. Configuring scan exclusions

Bitdefender allows excluding specific files, folders or file extensions from scanning. This feature is intended to avoid interference with your work and it can also help improve system performance. Exclusions are to be used by users having advanced computer knowledge or, otherwise, following the recommendations of a Bitdefender representative.

You can configure exclusions to apply to on-access or on-demand scanning only, or to both. The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.

Note

Exclusions will NOT apply for contextual scanning. Contextual scanning is a type of on-demand scanning: you right-click the file or folder you want to scan and select **Scan with Bitdefender**.

16.4.1. Excluding files or folders from scanning

To exclude specific files or folders from scanning, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module.
4. In the **Antivirus** window, select the **Exclusions** tab.
5. Turn on scan exclusions for files using the corresponding switch.
6. Click the **Excluded files and folders** link. In the window that appears, you can manage the files and folders excluded from scanning.
7. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, select the file or folder that you want to be excluded from scanning and then click **OK**. Alternatively, you can type (or copy and paste) the path to the file or folder in the edit field.
   c. By default, the selected file or folder is excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
   d. Click **Add**.
8. Click **OK** to save the changes and close the window.

16.4.2. Excluding file extensions from scanning

When you exclude a file extension from scanning, Bitdefender will no longer scan files with that extension, regardless of their location on your computer. The exclusion also applies to files on removable media, such as CDs, DVDs, USB storage devices or network drives.

> **Important**
> Use caution when excluding extensions from scanning because such exclusions can make your computer vulnerable to malware.

To exclude file extensions from scanning, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Click the **Antivirus** module.
4. In the **Antivirus** window, select the **Exclusions** tab.
5. Turn on scan exclusions for files using the corresponding switch.
6. Click the **Excluded extensions** link. In the window that appears, you can manage the file extensions excluded from scanning.
7. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Enter the extensions that you want to be excluded from scanning, separating them with semicolons (;). Here is an example:

      txt;avi;jpg

   c. By default, all files with the specified extensions are excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
   d. Click **Add**.
8. Click **OK** to save the changes and close the window.

16.4.3. Managing scan exclusions

If the configured scan exclusions are no longer needed, it is recommended that you delete them or disable scan exclusions.

To manage scan exclusions, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Exclusions** tab. Use the options in the **Files and folders** section to manage scan exclusions.
4. To remove or edit scan exclusions, click one of the available links. Proceed as follows:
   - To remove an entry from the table, select it and click the **Remove** button.
   - To edit an entry from the table, double-click it (or select it and click the **Edit** button). A new window appears where you can change the extension or the path to be excluded and the type of scanning you want them to

be excluded from, as needed. Make the necessary changes, then click **Modify**.

5. To turn off scan exclusions, use the corresponding switch.

16.5. Managing quarantined files

Bitdefender isolates the malware-infected files it cannot disinfect and the suspicious files in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

In addition, Bitdefender scans the quarantined files after each malware signature update. Cleaned files are automatically moved back to their original location.

To check and manage quarantined files, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Quarantine** tab.
4. Quarantined files are managed automatically by Bitdefender according to the default quarantine settings. Though not recommended, you can adjust the quarantine settings according to your preferences.

   Rescan quarantine after virus definitions update
   Keep this option turned on to automatically scan quarantined files after each virus definitions update. Cleaned files are automatically moved back to their original location.

   Submit suspicious quarantined files for further analysis
   Keep this option turned on to automatically send quarantined files to Bitdefender Labs. The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

   Delete content older than {30} days
   By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, type a new value in the

corresponding field. To disable automatic deletion of old quarantined files, type 0.

5. To delete a quarantined file, select it and click the **Delete** button. If you want to restore a quarantined file to its original location, select it and click **Restore**.

16.6. Active Threat Control

Bitdefender Active Threat Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Active Threat Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful and it is blocked automatically.

If Autopilot is off, you will be notified through a pop-up window about the blocked application. Otherwise, the application will be blocked without any notification. You can check what applications have been detected by Active Threat Control in the Events window.

16.6.1. Checking detected applications

To check the applications detected by Active Threat Control, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.
2. In the **Events** window, select **Antivirus** from the corresponding drop-down menu.
3. Click an event to view details about it.
4. If you trust the application, you can configure Active Threat Control not to block it anymore by clicking **Allow and monitor**. Active Threat Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

16.6.2. Turning on or off Active Threat Control

To turn on or off Active Threat Control, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module.
4. In the **Antivirus** window, select the **Shield** tab.
5. Click the switch to turn on or off Active Threat Control.

16.6.3. Adjusting the Active Threat Control protection

If you notice that Active Threat Control detects legitimate applications often, you should set a more permissive protection level.

To adjust the Active Threat Control protection, drag the slider along the scale to set the desired protection level.

Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Note

As you set the protection level higher, Active Threat Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

16.6.4. Managing excluded processes

You can configure exclusion rules for trusted applications so that Active Threat Control does not block them if they perform malware-like actions. Active Threat Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

To manage Active Threat Control process exclusions, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Exclusions** tab.

4. Click the **Excluded processes** link. In the window that appears, you can manage the Active Threat Control process exclusions.

   > **Note**
   > Process exclusions also apply to Intrusion Detection.

5. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
   c. Keep the **Allow** option selected to prevent Active Threat Control from blocking the application.
   d. Click **Add**.
6. To remove or edit exclusions, proceed as follows:
   - To remove an entry from the table, select it and click the **Delete** button.
   - To edit an entry from the table, double-click it (or select it) and click the **Modify** button. Make the necessary changes, then click **Modify**.
7. Save the changes and close the window.

17. ANTISPAM

Spam is a term used to describe unsolicited e-mail. Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving porn in your office mail) and you can't stop people from sending it. The next best thing to that is, obviously, to stop receiving it. Unfortunately, Spam comes in a wide range of shapes and sizes, and there's a lot of it.

Bitdefender Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox. For more information, please refer to "*Antispam insights*" (p. 107).

The Bitdefender Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server.

Note
Bitdefender does not provide antispam protection for e-mail accounts that you access through a web-based e-mail service.

The spam messages detected by Bitdefender are marked with the [spam] prefix in the subject line. Bitdefender automatically moves spam messages to a specific folder, as follows:

- In Microsoft Outlook, spam messages are moved to a **Spam** folder, located in the **Deleted Items** folder. The **Spam** folder is created during the installation of Bitdefender.
- In Outlook Express and Windows Mail, spam messages are moved directly to **Deleted Items**.
- In Mozilla Thunderbird, spam messages are moved to a **Spam** folder, located in the **Trash** folder. The **Spam** folder is created during the installation of Bitdefender.

If you use other mail clients, you must create a rule to move the e-mail messages marked as [spam] by Bitdefender to a custom quarantine folder.

17.1. Antispam insights

17.1.1. Antispam filters

The Bitdefender Antispam Engine incorporates cloud protection and other several different filters that ensure your Inbox to be SPAM-free, like Friends list, Spammers list and Charset filter.

Friends list / Spammers list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **friends or spammers list**, you can easily classify which people you want to receive e-mail from (friends) no matter what the message contains, or which people you never want to hear from again (spammers).

> **Note**
> We recommend that you add your friends' names and e-mail addresses to the **Friends list**. Bitdefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

Charset filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

17.1.2. Antispam operation

The Bitdefender Antispam Engine uses all antispam filters combined to determine whether a certain e-mail message should get into your **Inbox** or not.

Every e-mail that comes from the Internet is first checked with the Friends list/Spammers list filter. If the sender's address is found in the Friends list the e-mail is moved directly to your **Inbox**.

Otherwise, the Spammers list filter will take over the e-mail to verify if the sender's address is on its list. If a match is made, the e-mail will be tagged as SPAM and moved in the **Spam** folder.

Else, the Charset filter will check if the e-mail is written in Cyrillic or Asian characters. If so the e-mail will be tagged as SPAM and moved in the **Spam** folder.

Note
If the e-mail is tagged as SEXUALLY EXPLICIT in the subject line, Bitdefender will consider it SPAM.

17.1.3. Supported e-mail clients and protocols

Antispam protection is provided for all POP3/SMTP e-mail clients. The Bitdefender Antispam toolbar however is integrated only into:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express and Windows Mail (on 32-bit systems)
- Mozilla Thunderbird 3.0.4

17.2. Turning on or off antispam protection

Antispam protection is enabled by default.

To turn off the Antispam module, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antispam** module, then click the switch to turn on or off **Antispam**.

17.3. Using the antispam toolbar in your mail client window

In the upper area of your mail client window you can see the Antispam toolbar. The Antispam toolbar helps you manage antispam protection directly from your mail client. You can easily correct Bitdefender if it marked a legitimate message as SPAM.

Important
Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 108).

Each button from the Bitdefender toolbar will be explained below:

Settings - opens a window where you can configure the antispam filters and the toolbar settings.

Is Spam - indicates that the selected e-mail is spam. The e-mail will be moved immediately to the **Spam** folder. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.
Not Spam - indicates that the selected e-mail is not spam and Bitdefender should not have tagged it. The e-mail will be moved from the **Spam** folder to the **Inbox** directory. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.

Important
The **Not Spam** button becomes active when you select a message marked as SPAM by Bitdefender (normally these messages are located in the **Spam** folder).

Add Spammer - adds the sender of the selected e-mail to the Spammers list. You may need to click **OK** to acknowledge. The e-mail messages received from addresses in the Spammers list are automatically marked as [spam].
Add Friend - adds the sender of the selected e-mail to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
Spammers - opens the **Spammers list** that contains all the e-mail addresses from which you don't want to receive messages, regardless of their content. For more information, please refer to "*Configuring the Spammers List*" (p. 112).
Friends - opens the **Friends list** that contains all the e-mail addresses from which you always want to receive e-mail messages, regardless of their content. For more information, please refer to "*Configuring the Friends List*" (p. 111).

17.3.1. Indicating detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as [spam]). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the legitimate message incorrectly marked as [spam] by Bitdefender.
4. Click the **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge.

You will always receive e-mail messages from this address no matter what they contain.

5. Click the **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The e-mail message will be moved to the Inbox folder.

17.3.2. Indicating undetected spam messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

17.3.3. Configuring toolbar settings

To configure the antispam toolbar settings for your e-mail client, click **Settings** button on the toolbar and then the **Toolbar Settings** tab.

Here you have the following options:

- **Move message to Deleted Items** (only for Microsoft Outlook Express / Windows Mail)

  Note
  In Microsoft Outlook / Mozilla Thunderbird, detected spam messages are automatically moved to a Spam folder, located in the Deleted Items / Trash folder.

- **Mark spam e-mail messages as 'Read'** - marks the spam messages as read automatically, so as not to be disturbing when they arrive.
- You can choose whether or not to display confirmation windows when you click the **Add Spammer** and **Add Friend** buttons on the antispam toolbar.

  Confirmation windows can prevent accidentally adding e-mail senders to Friends / Spammers list.

17.4. Configuring the Friends List

The **Friends list** is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content. Messages from your friends are not labeled as spam, even if the content resembles spam.

> **Note**
> Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.

To configure and manage the Friends list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click the **Friends** button on the Bitdefender antispam toolbar.
- Alternatively, follow these steps:
  1. Click the icon in the lower-left corner of the Bitdefender interface.
  2. Select the **Protection** tab.
  3. Under the **Antispam** module, select **Manage Friends**.

To add an e-mail address, select the **E-mail address** option, enter the address and then click **Add**. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and then click **Add**. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will reach your **Inbox** regardless of their content;
- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will reach your **Inbox** regardless of their content;
- *com - all the received e-mail messages having the domain suffix com will reach your **Inbox** regardless of their content;

It is recommended to avoid adding entire domains, but this may be useful in some situations. For example, you can add the e-mail domain of the company you work for, or those of your trusted partners.

To delete an item from the list, click the corresponding **Remove** link. To delete all entries from the list, click the **Clear List** button.

You can save the Friends list to a file so that you can use it on another computer or after reinstalling the product. To save the Friends list, click the

Save button and save it to the desired location. The file will have a .bwl extension.

To load a previously saved Friends list, click the **Load** button and open the corresponding .bwl file. To reset the content of the existing list when loading a previously saved list, select **Overwrite current list**.

Click **OK** to save the changes and close the window.

17.5. Configuring the Spammers List

The **Spammers list** is a list of all the e-mail addresses from which you don't want to receive messages, regardless of their content. Any e-mail message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.

To configure and manage the Spammers list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click **Spammers** button on the Bitdefender antispam toolbar integrated into your mail client.
- Alternatively, follow these steps:
  1. Click the icon in the lower-left corner of the Bitdefender interface.
  2. Select the **Protection** tab.
  3. Under the **Antispam** module, select **Manage Spammers**.

To add an e-mail address, select the **E-mail address** option, enter the address and then click **Add**. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and then click **Add**. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will be tagged as SPAM;
- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will be tagged as SPAM;
- *com - all the received e-mail messages having the domain suffix com will be tagged as SPAM.

It is recommended to avoid adding entire domains, but this may be useful in some situations.

Warning

Do not add domains of legitimate web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) to the Spammers list. Otherwise, the e-mail messages received from any registered user of such a service will be detected as spam. If, for example, you add yahoo.com to the Spammers list, all e-mail messages coming from yahoo.com addresses will be marked as [spam].

To delete an item from the list, click the corresponding **Remove** link. To delete all entries from the list, click the **Clear List** button.

You can save the Spammers list to a file so that you can use it on another computer or after reinstalling the product. To save the Spammers list, click the **Save** button and save it to the desired location. The file will have a .bwl extension.

To load a previously saved Spammers list, click the **Load** button and open the corresponding .bwl file. To reset the content of the existing list when loading a previously saved list, select **Overwrite current list**.

Click **OK** to save the changes and close the window.

17.6. Configuring the local antispam filters

As described in "*Antispam insights*" (p. 107), Bitdefender uses a combination of different antispam filters to identify spam. The antispam filters are pre-configured for efficient protection.

Important

Depending on whether or not you receive legitimate e-mails written in Asian or Cyrillic characters, disable or enable the setting that automatically blocks such e-mails. The corresponding setting is disabled in the localized versions of the program that use such charsets (for example, in the Russian or Chinese version).

To configure the local antispam filters, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antispam** module, then click the switches to turn on or off the local antispam filters.

If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, you can configure the local antispam filters directly from your mail client. Click the **Settings** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window) and then the **Antispam Filters** tab.

17.7. Configuring the cloud settings

The cloud detection makes use of the Bitdefender Cloud services to provide you with efficient and always up-to-date antispam protection.

The cloud protection functions as long as you keep Bitdefender Antispam enabled.

Samples of legitimate or spam e-mails can be submitted to Bitdefender Cloud when you indicate detection errors or undetected spam e-mails. This helps improve the Bitdefender antispam detection.

Configure the e-mail sample submission to Bitdefender Cloud by selecting the desired options, by following these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antispam** module, then select the desired options from the **Settings** tab.

If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, you can configure the cloud detection directly from your mail client. Click the **Settings** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window) and then the **Cloud Settings** tab.

18. WEB PROTECTION

Bitdefender Web Protection ensures a safe browsing experience by alerting you about potential phishing web pages.

Bitdefender provides real-time web protection for:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

To configure Web Protection settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Web Protection** module.

Click the switches to turn on or off:

- Search Advisor, a component that rates the results of your search engine queries and the links posted on social networking websites by placing an icon next to every result:

  You should not visit this web page.

  This web page may contain dangerous content. Exercise caution if you decide to visit it.

  This is a safe page to visit.

  Search Advisor rates the search results from the following web search engines:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor rates the links posted on the following online social networking services:
  - Facebook
  - Twitter

- Scanning SSL web traffic.

More sophisticated attacks might use secure web traffic to mislead their victims. It is therefore recommended to enable SSL scanning.

- Protection against fraud.
- Protection against phishing.

You can create a list of web sites that will not be scanned by the Bitdefender antimalware, antiphishing and antifraud engines. The list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.

To configure and manage web sites using the web protection provided by Bitdefender, click the **Whitelist** link. A new window appears.

To add a site to the whitelist, provide its address in the corresponding field and click **Add**.

To remove a web site from the list, select it in the list and click the corresponding **Remove** link.

Click **Save** to save the changes and close the window.

18.1. Bitdefender alerts in the browser

Whenever you try to visit a website classified as unsafe, the website is blocked and a warning page is displayed in your browser.

The page contains information such as the website URL and the detected threat.

You have to decide what to do next. The following options are available:

- Navigate away from the web page by clicking **Take me back to safety**.
- Disable blocking pages that contain phishing by clicking **Disable Antiphishing filter**.
- Disable blocking pages that contain malware by clicking **Disable Antimalware filter**.
- Add the page to the Antiphishing whitelist by clicking **Add to whitelist**. The page will no longer be scanned by Bitdefender Antiphishing engines.
- Proceed to the web page, despite the warning, by clicking **I understand the risks, take me there anyway**.

19. DATA PROTECTION

19.1. Deleting files permanently

When you delete a file, it can no longer be accessed through normal means. However, the file continues to be stored on the hard disk until it is overwritten when copying new files.

The Bitdefender File Shredder helps you permanently delete data by physically removing it from your hard disk.

You can quickly shred files or folders from your computer using the Windows contextual menu, by following these steps:

1. Right-click the file or folder you want to permanently delete.
2. Select **Bitdefender** > **File Shredder** in the context menu that appears.
3. A confirmation window appears. Click **Yes** to start the File Shredder wizard.
4. Wait for Bitdefender to finish shredding the files.
5. The results are displayed. Click **Close** to exit the wizard.

Alternatively, you can shred files from the Bitdefender interface.

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Under the **Data Protection** module, select **File Shredder**.
4. Follow the File Shredder wizard:
   a. **Add Folder(s)**

      Add the files or folders you want to be permanently removed.
   b. Click **Next** and confirm that you wish to continue with the process.

      Wait for Bitdefender to finish shredding the files.
   c. **Results**

      The results are displayed. Click **Close** to exit the wizard.

20. FILE ENCRYPTION

Bitdefender File Encryption enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. The data stored on the vaults can only be accessed by users who know the password.

The password allows you to open, store data on and close a vault while maintaining its security. While a vault is open, you can add new files, access current files or change them.

Physically, the vault is a file stored on the local hard drive having the .bvd extension. Although the physical files representing the vaulted drives can be accessed from a different operating system (such as Linux), the information stored on them cannot be read because it is encrypted.

File vaults can be managed from the Bitdefender window or by using the Windows contextual menu and logical drive associated with the vault.

20.1. Managing file vaults

To manage your file vaults from Bitdefender, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.

   The existing file vaults appear in the My Vaults window.

20.2. Creating file vaults

To create a new vault:

1. Click the **Add** button.
2. In the **Start fresh** area, click **Create new**.
3. Specify the location and the name of the vault file.
   - Click **Browse**, select the location of the vault and save the vault file under the desired name.
   - Type the name of the vault file on the disk in the corresponding fields.

4. Choose a drive letter from the corresponding menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in My Computer.
5. If you want to change the default size (100 MB) of the vault, type the desired value in the **Vault size (MB)** field.
6. Type the desired password to the vault in the **Password** and **Confirm password** fields. The password must have at least 8 characters. Anyone trying to open the vault and access its files must provide the password.
7. Click **Create**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

To create quicker a new vault, right-click on your desktop or in a folder on your computer, point to **Bitdefender** > **Bitdefender File Vault** and select **Create File Vault**.

Note
It may be convenient to save all file vaults to the same location. In this way, you can find them quicker.

20.3. Opening file vaults

In order to access and work with the files stored in a vault, you must open the vault. When you open the vault, a virtual disk drive appears in My Computer. The drive is labeled with the drive letter assigned to the vault.

To open a vault, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.
4. In the **My Vaults** window, select the vault you want to open.
5. Click the **Unlock** button, and type the required password.
6. Click the **Open** button to open your vault.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

To open quicker a vault, locate on your computer the .bvd file representing the vault you want to open. Right-click the file, point to **Bitdefender File Vault** and select **Open**. Type the required password, and then click **OK**.

20.4. Adding files to vaults

Before you can add files or folders to a vault, you must open the vault.

To add new files to your vault, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.
4. In the **My Vaults** window, select the vault you want to open.
5. Click the **Unlock** button, and type the required password.
6. Click the **Open** button to open your vault.
7. Add files or folders as you normally do in Windows (for example, you can use the copy-and-paste method).

To add quicker files to your vault, right-click the file or folder you want to copy to a vault, point to **Bitdefender File Vault** and click **Add to File Vault**.

- If only one vault is open, the file or folder is copied directly to that vault.
- If several vaults are open, you will be prompted to choose the vault to copy the item to. Select from the menu the drive letter corresponding to the desired vault and click **OK** to copy the item.

20.5. Locking vaults

When you are done with your work in a file vault, you must lock it in order to protect your data. By locking the vault, the corresponding virtual disk drive disappears from My Computer. Consequently, access to the data stored in the vault is completely blocked.

To lock a vault, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.

4. In the **My Vaults** window, select the vault you want to lock.
5. Click the **Lock** button.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

To lock quicker a vault, right-click the .bvd file representing the vault, point to **Bitdefender File Vault** and click **Lock**.

20.6. Removing files from vaults

In order to remove files or folders from a vault, the vault must be open. To remove files or folders from a vault, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.
4. In the **My Vaults** window, select the vault from which you want to remove files.
5. Click the **Unlock** button, in case it is locked.
6. Click the **Open** button.

   Remove files or folders as you normally do in Windows (for example, right-click a file you want to delete and select **Delete**).

20.7. Changing vault password

The password protects the content of a vault from unauthorized access. Only users who know the password can open the vault and access the documents and data stored inside it.

The vault must be locked before you can change its password. To change the password of a vault, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **File Encryption** module.
4. In the **My Vaults** window, select the vault for which you want to change the password.

5. Click the **Settings** button.
6. Type the current password of the vault in the **Old Password** field.
7. Type the new password of the vault in the **New Password** and **Confirm New Password** fields.

> **Note**
> The password must have at least 8 characters. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

To change quicker the password of a vault, locate on your computer the .bvd file representing the vault. Right-click the file, point to **Bitdefender File Vault** and select **Change Vault Password**.

21. VULNERABILITY

An important step in protecting your computer against malicious persons and applications is to keep up to date the operating system and the applications you regularly use. You should also consider disabling Windows settings that make the system more vulnerable to malware. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account.

Bitdefender automatically checks your system for vulnerabilities and alerts you about them. System vulnerabilities include the following:

- outdated applications on your computer.
- missing Windows updates.
- weak passwords to Windows user accounts.

Bitdefender provides two easy ways to fix the vulnerabilities of your system:

- You can scan your system for vulnerabilities and fix them step by step using the **Vulnerability Scan** option.
- Using automatic vulnerability monitoring, you can check and fix detected vulnerabilities in the Events window.

You should check and fix system vulnerabilities every one or two weeks.

21.1. Scanning your system for vulnerabilities

To fix system vulnerabilities using the Vulnerability Scan option, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Vulnerability** module, select **Vulnerability Scan**.
4. Wait for Bitdefender to check your system for vulnerabilities. To stop the scanning process, click the **Skip** button at the top of the window.

   Or quicker, click the **Vulnerability Scan** action button from the Bitdefender interface.

   - **Critical Windows updates**

Click **View details** to see the list of critical Windows updates that are not currently installed on your computer.

To initiate the installation of selected updates, click **Install updates**. Please note that it may take a while to install the updates and some of them may require a system restart to complete the installation. If required, restart the system at your earliest convenience.

- **Application updates**

  If an application is not up to date, click the **Download new version** link to download the latest version.

  Click **View details** to see information about the application that needs to be updated.

- **Weak Windows account passwords**

  You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides.

  Click **Change password at login** to set a new password for your system.

  Click **View details** to modify the weak passwords. You can choose between asking the user to change the password at the next login or changing the password yourself immediately. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

In the upper-right corner of the window you can filter the results according to your preferences.

21.2. Using automatic vulnerability monitoring

Bitdefender scans your system for vulnerabilities regularly, in the background, and keeps records of detected issues in the Events window.

To check and fix the detected issues, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Events** from the drop-down menu.
2. In the **Events** window, select **Vulnerability** from the Select Events list.
3. You can see detailed information regarding the detected system vulnerabilities. Depending on the issue, to fix a specific vulnerability proceed as follows:

- If Windows updates are available, click **Update now**.
- If automatic Windows update is disabled, click **Enable**.
- If an application is outdated, click **Update now** to find a link to the vendor web page from where you can install the latest version of that application.
- If a Windows user account has a weak password, click **Change password** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
- If the Windows Autorun feature is enabled, click **Fix** to disable it.

To configure the vulnerability monitoring settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Vulnerability** module.
4. Click the switch to turn on or off Vulnerability scan.

   Important
   To be automatically notified about system or application vulnerabilities, keep the **Vulnerability scan** option enabled.

5. Choose the system vulnerabilities you want to be regularly checked by using the corresponding switches.

   Critical Windows updates
   Check if your Windows operating system has the latest critical security updates from Microsoft.

   Application updates
   Check if applications installed on your system are up-to-date. Outdated applications can be exploited by malicious software, making your PC vulnerable to outside attacks.

   Weak passwords
   Check whether the passwords of the Windows accounts configured on the system are easy to guess or not. Setting passwords that are hard to guess (strong passwords) makes it very difficult for hackers

to break into your system. A strong password includes uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

Media autorun

Check the status of the Windows Autorun feature. This feature enables applications to be automatically started from CDs, DVDs, USB drives or other external devices.

Some types of malware use Autorun to spread automatically from removable media to the PC. This is why it is recommended to disable this Windows feature.

Note

If you turn off monitoring of a specific vulnerability, related issues will no longer be recorded in the Events window.

22. FIREWALL

The Firewall protects your computer from inbound and outbound unauthorized connection attempts, both on local networks and on the Internet. It is quite similar to a guard at your gate - it keeps track of connection attempts and decides which to allow and which to block.

The Bitdefender firewall uses a set of rules to filter data transmitted to and from your system. The rules are grouped into 2 categories:

General Rules

Rules that determine the protocols over which communication is allowed.

A default set of rules that provides an optimal protection is used. You can edit the rules by allowing or denying connections over certain protocols.

Application Rules

Rules that determine how each application can access network resources and the Internet.

Under normal conditions, Bitdefender automatically creates a rule whenever an application tries to access the Internet. You can also manually add or edit rules for applications.

Bitdefender automatically assigns a network type to every network connection it detects. Depending on the network type, the firewall protection is set to the appropriate level for each connection.

To find out more about the firewall settings for each network type and how you can edit the network settings, please refer to "*Managing connection settings*" (p. 131).

22.1. Turning on or off firewall protection

To turn firewall protection on or off, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Firewall** module, then click the Firewall switch.

Warning

Because it exposes your computer to unauthorized connections, turning off the firewall should only be a temporary measure. Turn the firewall back on as soon as possible.

22.2. Managing firewall rules

22.2.1. General rules

Whenever data is transmitted over the Internet, certain protocols are used.

The general rules allow you to configure the protocols over which traffic is allowed. By default, general rules are not displayed when you open Firewall. To edit the rules, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Firewall** module.
4. In the **Firewall** window, select the **Rules** tab.
5. Check the **Show general rules** box in the left-lower corner of the window.

The default rules are displayed. To edit the priority of a rule, click the corresponding arrow in the **Permission** column and select **Allow** or **Deny**.

DNS over UDP / TCP
Allow or deny DNS over UDP and TCP.

By default, this type of connection is allowed.

Sending E-mails
Allow or deny sending e-mails over SMTP.

By default, this type of connection is allowed.

Web Browsing HTTP
Allow or deny HTTP web browsing.

By default, this type of connection is allowed.

Incoming ICMP / ICMPv6
Allow or deny ICMP / ICMPv6 messages.

ICMP messages are often used by hackers to carry out attacks against computer networks. By default, this type of connection is denied.

Incoming Remote Desktop Connections
Allow or deny other computers' access over Remote Desktop Connections.

By default, this type of connection is allowed.

Windows Explorer traffic on HTTP / FTP
Allow or deny HTTP and FTP traffic from Windows Explorer.

By default, this type of connection is denied.

22.2.2. Application rules

To view and manage the firewall rules controlling applications' access to network resources and the Internet, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Firewall** module.
4. In the **Firewall** window, select the **Rules** tab.

You can see the programs (processes) for which firewall rules have been created in the table. To see the rules created for a specific application, simply double-click it.

For each rule the following information is displayed:

- **Name** - the name of the process the rules applies to.
- **Network Type** - the process and the network adapter types the rule applies to. Rules are automatically created to filter network or Internet access through any adapter. By default, the rules apply to any network. You can manually create rules or edit existing rules to filter an application's network or Internet access through a specific adapter (for example, a wireless network adapter).
- **Protocol** - the IP protocol the rule applies to. By default, the rules apply to any protocol.
- **Permission** - whether the application is allowed or denied access to the network or Internet under the specified circumstances.

To manage the rules, use the buttons above the table:

- **Add rule** - opens a window where you can create a new rule.

- **Remove rule** - deletes the selected rule.
- **Reset rules** - opens a window where you can choose to remove the current set of rules and restore the default ones.

Adding / editing application rules

To add or edit an application rule, click the **Add rule** button above the table or click a current rule. A new window appears. Proceed as follows:

In the **Settings** tab you can apply the following changes:

- **Program Path.** Click **Browse** and select the application the rule applies to.
- **Network Type.** Select the type of network the rule applies to. You can change the type by opening the **Network Type** drop-down menu and selecting one of the available types from the list.

Network Type	Description
Trusted	Disable the firewall for the respective adapter.
Home/Office	Allow all traffic between your computer and computers in the local network.
Public	All traffic is filtered.
Untrusted	Completely block network and Internet traffic through the respective adapter.

- **Permission.** Select one of the available permissions:

Permission	Description
Allow	The specified application will be allowed network / Internet access under the specified circumstances.
Deny	The specified application will be denied network / Internet access under the specified circumstances.

In the **Advanced** tab you can customize the following settings:

- **Custom Local Address.** Specify the local IP address and port the rule applies to.

- **Custom Remote Address.** Specify the remote IP address and port the rule applies to.
- **Direction.** Select from the menu the traffic direction the rule applies to.

Direction	Description
Outbound	The rule applies only for the outgoing traffic.
Inbound	The rule applies only for the incoming traffic.
Both	The rule applies in both directions.

- **Protocol.** Select from the menu the IP protocol the rule applies to.
  - If you want the rule to apply to all protocols, select **Any**.
  - If you want the rule to apply to TCP, select **TCP**.
  - If you want the rule to apply to UDP, select **UDP**.
  - If you want the rule to apply to a specific protocol, type the number assigned to the protocol you want to filter in the blank edit field.

> **Note**
>
> IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers.

22.3. Managing connection settings

For each network connection you can configure special trusted or untrusted zones.

A trusted zone is a device that you fully trust, for example a computer or a printer. All traffic between your computer and a trusted device is allowed. To share resources with specific computers in an unsecured wireless network, add them as allowed computers.

An untrusted zone is a device that you do not want to communicate with your computer at all.

To view and manage zones on your network adapters, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Click the **Firewall** module.
4. In the **Firewall** window, select the **Adapters** tab.

The network adapters with active connections and the current zones, if any, are displayed in this tab.

For each zone the following information is displayed:

- **Network Type** - the type of network your computer is connected to.
- **Stealth Mode** - whether you can be detected by other computers.

  To configure the Stealth Mode, select the desired option from the corresponding drop-down menu.

Stealth option	Description
On	Stealth Mode is on. Your computer is invisible from both the local network and the Internet.
Off	Stealth Mode is off. Anyone from the local network or the Internet can ping and detect your computer.

- **Generic** - whether generic rules are applied to this connection.

  If the IP address of a network adapter is changed, Bitdefender modifies the network type accordingly. If you want to keep the same type, select **Yes** from the corresponding drop-down menu.

Adding / editing exceptions

To add or edit an exception, click the **Network exceptions** button above the table. A new window displaying the available Adapters connected to the network will appear. Proceed as follows:

1. Select the IP address of the computer you want to add, or type an address or address range in the provided text box.
2. Select the permission:
   - **Allow** - to allow all traffic between your computer and the selected computer.

- **Deny** - to block all traffic between your computer and the selected computer.

3. Click the + button to add the exception and close the window.

   If you want to remove an IP, click the corresponding button and close the window.

22.4. Configuring advanced settings

To configure advanced firewall settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Firewall** module.
4. In the **Firewall** window, select the **Settings** tab.

The following feature can be enabled or disabled.

- **Block port scans in the network** - detects and blocks attempts to find out which ports are open.

  Port scans are frequently used by hackers to find out which ports are open on your computer. They might then break into your computer if they find a less secure or vulnerable port.

22.5. Configuring alert intensity

Bitdefender Total Security 2016 was designed to be as unintrusive as possible. Under normal conditions, you do not have to make decisions on whether to allow or deny connections or actions attempted by the applications running on your system.

If you want to be in complete control of the decision making, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window select the **General Settings** tab.
3. Turn on **Paranoid mode** by clicking the corresponding switch.

Note

When Paranoid mode is turned on, the Autopilot and Profiles features are automatically switched off.
Paranoid mode can be used simultaneously with **Battery Mode**.

As long as Paranoid mode is on, you will be prompted for action every time one of the following situations occurs:

- An application tries to connect to the Internet.
- An application tries to perform an action considered suspicious by the Intrusion Detection or the Active Threat Control.

The alert contains detailed information regarding the application and the detected behavior. Select to **Allow** or **Deny** the action using the corresponding button.

23. INTRUSION DETECTION

Bitdefender Intrusion Detection monitors the network and system activities for malicious activities or policy violations. It can detect and block attempts to change critical system files, Bitdefender files or registry entries, the installation of malware drivers and attacks performed by code injection (DLL injection).

To configure the Intrusion Detection, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Intrusion Detection** module.
4. To turn on the Intrusion Detection, click the corresponding switch.
5. Drag the slider along the scale to set the desired aggressiveness level. Use the description on the right side of the scale to choose the level that better fits your security needs.

You can check what applications have been detected by the Intrusion Detection in the Events window.

If there are applications you trust and do not want the Intrusion Detection to scan, you can add exclusion rules for them. To exclude an application from scanning, follow the steps described in section "*Managing excluded processes*" (p. 104).

Note

The operation of the Intrusion Detection is related to that of the Active Threat Control. Process exclusion rules apply to both systems.

24. RANSOMWARE PROTECTION

Ransomware is a malicious software that attacks vulnerable systems by locking them, and asks for money to let the user take back the control of his system. This malicious software acts intelligent by displaying false messages to panic the user, urging him to proceed with the asked payment.

The infection can be spread via spam e-mails, by downloading attachments, or by visiting infected websites and installing malicious applications without letting the user know what is happening on his system.

Ransomware can have one of the following behaviors preventing the user from accessing his system:

- Encrypts sensitive and personal files without giving the possibility of decryption until a ransom is paid by the victim.
- Locks the computer's screen and displays a message asking for money. In this case, no file is encrypted, only the user is forced to proceed with the payment.
- Blocks applications from running.

Using the latest technology, Bitdefender Ransomware Protection ensures system integrity by protecting critical system areas against damages without impacting the system. However, you may also want to protect your personal files such as documents, photos, movies, or the files you keep stored in the cloud.

24.1. Turning on or off Ransomware Protection

To turn off the Ransomware Protection module, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click **Ransomware Protection**.
4. Click the switch to turn on or off **Ransomware Protection**.

Each time an application will try to access a protected file, a Bitdefender pop-up is displayed. You can allow or deny the access.

24.2. Protect personal files from ransomware attacks

If you want to settle personal files to a shelter, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Ransomware Protection** module, then click the **Protected Folders** button.
4. Click **Add**, and then go to the folder you want to protect.
5. Click **OK** to add the selected folder to the protection environment.

By default, the folders My Documents, My Pictures, Public documents, and Public Pictures are protected against malware attacks. Personal data stored in online file hosting services such as Box, Dropbox, Google Drive, and OneDrive are also included to the protection environment, provided that their applications are installed on the system.

Note
Custom folders can be protected only for current users. System and application files cannot be added to exceptions.

24.3. Configuring trusted applications

Disable ransomware protection for specific applications, but only the ones you trust should be added to the list.

To add trusted applications to exclusions, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Ransomware Protection** module, select **Trusted applications**.
4. Click **Add** and browse to the applications you want to protect.
5. Click **OK** to add the selected application to the protection environment.

24.4. Configuring blocked applications

Among the applications you have installed on your computer, some may want to access your personal files.

To restrict those applications, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Ransomware Protection** module, select **Blocked applications**.
4. Click **Add** and browse to the applications you want to restrict.
5. Click **OK** to add the selected application to the restricted list.

24.5. Protection at boot

It is known that many malware applications are set to run at system startup, a fact which can seriously damage a machine. Bitdefender Boot time protection scans all critical system areas before all files are being loaded, with zero impact on the system. At the same time, protection is provided from certain attacks that rely on stack or heap code execution, code injections or hooks inside certain core dynamic libraries.

To disable Protection at boot, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click **Ransomware Protection**.
4. Click the switch to turn on or off **Protection at boot**.

25. SAFEPAY SECURITY FOR ONLINE TRANSACTIONS

The computer is fast becoming the main tool for shopping and banking. Paying bills, transferring money, buying pretty much anything you can imagine has never been quicker or easier.

This involves sending personal information, account and credit card data, passwords and other types of private information over the Internet, in other words exactly the type of information flow that cyber-criminals are very interested to tap into. Hackers are relentless in their efforts to steal this information, so you can never be too careful about securing online transactions.

Bitdefender Safepay™ is first of all a protected browser, a sealed environment that is designed to keep your online banking, e-shopping and any other type of online transaction private and secure.

For the best privacy protection, Bitdefender Password Manager has been integrated into Bitdefender Safepay™ to secure your credentials whenever you want to access private online locations. For more information, please refer to "*Password Manager protection for your credentials*" (p. 144).

Bitdefender Safepay™ offers the following features:

- It blocks access to your desktop and any attempt to take snapshots of your screen.
- It protects your secret passwords while browsing online with Password Manager.
- It comes with a virtual keyboard which, when used, makes it impossible for hackers to read your keystrokes.
- It is completely independent from your other browsers.
- It comes with built-in hotspot protection to be used when your computer is connected to unsecured Wi-fi networks.
- It supports bookmarks and allows you to navigate between your favorite banking/shopping sites.
- It is not limited to banking and e-shopping. Any website can be opened in Bitdefender Safepay™.

25.1. Using Bitdefender Safepay™

By default, Bitdefender detects when you navigate to an online banking site or online shop in any browser on your computer and prompts you to launch it in Bitdefender Safepay™.

To access the main interface of Bitdefender Safepay™, use one of the following methods:

- From the Bitdefender interface:
  1. Click the **Safepay** action button from the Bitdefender interface.
- From Windows:
  - In **Windows 7**:
    1. Click **Start** and go to **All Programs**.
    2. Click **Bitdefender**.
    3. Click **Bitdefender Safepay™**.
  - In **Windows 8 and Windows 8.1**:

    Locate Bitdefender Safepay™ from the Windows Start screen (for example, you can start typing "Bitdefender Safepay™" directly in the Start screen) and then click the icon.
  - In **Windows 10**:

    Type "Bitdefender Safepay™" in the search box from the taskbar and click its icon.

Note
If the Adobe Flash Player plugin is not installed or is outdated, a Bitdefender message will be displayed. Click the corresponding button to continue.
After the installation process is completed, you will have to manually reopen the Bitdefender Safepay™ browser to continue your work.

If you are used to web browsers, you will have no trouble using Bitdefender Safepay™ - it looks and behaves like a regular browser:

- enter URLs you want to go to in the address bar.
- add tabs to visit multiple websites in the Bitdefender Safepay™ window by clicking .
- navigate back and forward and refresh pages using respectively.

- access Bitdefender Safepay™ settings by clicking and choosing **Settings**.
- protect your passwords with Password Manager by clicking .
- manage your bookmarks by clicking next to the address bar.
- open the virtual keyboard by clicking .
- increase or decrease the browser size by pressing simultaneously **Ctrl** and the **+/-** keys in the numeric keypad.
- view information about your Bitdefender product by clicking and choosing **About**.
- print important information by clicking .

25.2. Configuring settings

Click and choose **Settings** to configure Bitdefender Safepay™:

General Settings

Choose what will happen when you access an online shop or Internet banking site in your regular web browser:

- Automatically open websites in Safepay.
- Recommend me to use Safepay.
- Do not recommend me to use Safepay.

Domains list

Choose how Bitdefender Safepay™ will behave when you visit websites from specific domains in your regular web browser by adding them to the domains list and selecting the behavior for each one:

- Automatically open in Bitdefender Safepay™.
- Have Bitdefender prompt you for action each time.
- Never use Bitdefender Safepay™ when visiting a page from the domain in a regular browser.

Blocking pop-ups

You can choose to block pop-ups by clicking the corresponding switch.

You can also create a list of web sites to allow pop-ups from. The list should contain only web sites you fully trust.

To add a site to the list, provide its address in the corresponding field and click **Add domain**.

To remove a web site from the list, select it in the list and click the corresponding **Remove** link.

Enable Hotspot protection

You can enable an extra layer of protection when connected to unsecured Wi-fi networks by enabling this feature.

Access "*Hotspot protection for unsecured networks*" (p. 142) for more information.

25.3. Managing bookmarks

If you disabled the automatic detection of some or all websites, or Bitdefender simply doesn't detect certain websites, you can add bookmarks to Bitdefender Safepay™ so that you can easily launch favorite websites in the future.

Follow these steps to add a URL to Bitdefender Safepay™ bookmarks:

1. Click the icon next to the address bar to open the Bookmarks page.

   Note
   The Bookmarks page is opened by default when you start Bitdefender Safepay™.

2. Click the **+** button to add a new bookmark.
3. Enter the URL and the title of the bookmark and click **Create**. Check the **Automatically open in Safepay** option if you want the bookmarked page to open with Bitdefender Safepay™ each time you access it. The URL is also added to the Domains list on the settings page.

25.4. Hotspot protection for unsecured networks

When using Bitdefender Safepay™ while connected to unsecured Wi-fi networks (for example, a public hotspot) an extra layer of security is offered by the Hotspot protection feature. This service encrypts Internet communication over unsecured connections, helping you maintain your privacy no matter what network you are connected to.

The Hotspot protection works only if your computer is connected to an unsecured network.

The secure connection will be initialized and a message will be displayed in the Bitdefender Safepay™ window when the connection is established. The

symbol appears in front of the URL in the address bar to help you easily identify secure connections.

To improve your visual browsing experience, you can choose to enable **Adobe Flash** and **Java** plugins by clicking **Show advanced settings**.

You may need to acknowledge the action.

26. PASSWORD MANAGER PROTECTION FOR YOUR CREDENTIALS

We use our computers to shop online or pay our bills, to connect to social media platforms or log in with instant messaging applications.

But as everybody knows, it's not always easy to remember the password!

And if we are not careful while browsing online, our private information, such as our e-mail address, our instant messaging ID or our credit card data can be compromised.

To keep your passwords or your personal data on a sheet of paper or in the computer can be dangerous because they can be accessed and used by people who want to steal and use that information. And to remember each password you have set for your online accounts or for your favorite websites is not an easy task.

Therefore, is there a way to make sure that we find our passwords when we need them? And can we rest assured that our secret passwords are always safe?

Password Manager helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

Using a single master password to access your credentials, Password Manager makes it easy for you to keep your passwords safe in a Wallet.

To offer the best protection for your online activities, Password Manager is integrated with Bitdefender Safepay™ and provides a unified solution for the various ways in which your private data can be compromised.

Password Manager protects the following private information:

- Personal information, such as the e-mail address or the phone number
- Login credentials for the websites
- Bank account information or the credit card number
- Access data to the e-mail accounts
- Passwords for the applications
- Passwords for the Wi-Fi networks

26.1. Configuring the Password Manager

Once the installation is finished and you open your browser, you will be notified through a pop-up window that you can use Wallet for an easier browsing experience.

Bitdefender Wallet is the place where you can store your personal data.

Click **Explore** to start the setup wizard for the Wallet. Follow the wizard to complete the setup process.

Two tasks can be performed during this step:

- Create a new Wallet database to protect your passwords.

  During the setup process, you will be asked to protect your Wallet with a master password. The password should be strong and contain at least 7 characters.

  To create a strong password use minimum one number or symbol, and one upper case character. Once you have set a password, anyone trying to access the Wallet will first have to provide the password.

  After setting the master password, you are given the possibility to synchronize the Wallet information in the cloud so you can use it on all your devices.

  At the end of the setup process, the following Wallet settings are enabled by default:

  - **Save credentials automatically in Wallet**.
  - **Ask for my master password when I login to my computer**.
  - **Automatically lock Wallet when I leave my PC unattended**.
- Import an existing database if you previously used Wallet on your system.

Export the Wallet database

To export your Wallet database, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Wallets** tab.

4. Select the desired Wallet database from the **My Wallets** section, then click the **Export** button.
5. Follow the steps to export the Wallet database to a location on your system.

Note
The Wallet needs to be opened in order for the **Export** button to be available.

Create a new Wallet database

To create a new Wallet database, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Wallets** tab.
4. Click the + icon in the window that appears.
5. In the **Start Fresh** area, click **Create New**.
6. Type the required information in the corresponding fields.
   - Wallet label - type a unique name for your Wallet database.
   - Master Password - type a password for your Wallet.
   - Retype Password - retype the password you set.
   - Hint - type a hint to remember the password.
7. Click **Continue**.
8. At this step you can choose to store your information in the cloud. If you select Yes, banking information will remain stored locally on your device. Choose the desired option, then click **Continue**.
9. Select the web browser you want to import credentials from.
10. Click **Finish**.

Synchronize your wallets in the cloud

To turn the wallets synchronization in the cloud on or off, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Wallets** tab.
4. Select the desired Wallet database from the **My Wallets** section, then click the **Settings** button.
5. Choose the desired option in the window that appears, then click **Save**.

Note
The Wallet needs to be opened in order for the **Settings** button to be available.

Manage your Wallet credentials

To manage your passwords, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Wallets** tab.
4. Select the desired Wallet database from the **My Wallets** section, then click the **Open** button.

A new window appears. Select the desired category from the upper part of the window:

- Identity
- Websites
- Online banking
- Emails
- Applications
- Wi-Fi Networks

Adding/ editing the credentials

- To add a new password, choose the desired category from the top, click **+ Add item**, insert the information in the corresponding fields and click the Save button.
- To edit an entry from the table, select it and click the **Edit** button.
- To exit, click **Cancel**.

- To remove an entry, select it, click the **Edit** button and choose **Delete**.

26.2. Turning on or off the Password Manager protection

To turn the Password Manager protection on or off, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module.
4. Click the **Module status** switch to turn Password Manager on or off.

26.3. Managing the Password Manager settings

To configure the master password in detail, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Security Settings** tab.

The following options are available:

- **Ask for my master password when I login to my PC** - you will be prompted to insert your master password when you access the computer.
- **Ask for my master password when I open my browsers and apps** - you will be prompted to insert your master password when you access a browser or an application.
- **Automatically lock Wallet when I leave my PC unattended** - you will be prompted to insert your master password when you return to your computer after 15 minutes.

Important

Be sure to remember your master password or keep a record of it in a safe place. If you forget the password, you will have to reinstall the program or contact Bitdefender for support.

Improve your experience

To select the browsers or the applications where you want to integrate Password Manager, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Plugins** tab.

   Check an application to use Password Manager and improve your experience:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Skype
   - Yahoo! Messenger

Configuring the Autofill

The Autofill feature makes it easy for you to connect with your favorite websites or to log in with your online accounts. The first time you enter your login credentials and personal information into your web browser, they are automatically secured into the Wallet.

To configure the **Autofill** settings, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Click the **Password Manager** module, then select the **Autofill settings** tab.
4. Configure the following options:
   - **Autofill login credentials**:
     - **Autofill login credentials every time** - the credentials are inserted automatically into the browser.

- **Let me choose when I want to autofill my login credentials** - you can choose when to autofill the credentials into the browser.

- **Configure how Password Manager secures your credentials**:
  - **Save credentials automatically in Wallet** - the login credentials and other identifiable information such as your personal and credit card details are automatically saved and updated into the Wallet.
  - **Ask me every time** - you will be asked every time if you want to add your credentials to the Wallet.
  - **Do not save, I will update the information manually** - the credentials can be added only manually into the Wallet.
- **Autofill forms**:
  - **Prompt my fill options when I visit a page with forms** - a popup with the fill options will appear every time Bitdefender detects that you want to perform an online payment or to sign up.

Manage the Password Manager information from your browser

You can easily manage the Password Manager details directly from your browser, to have all the important data at hand. The Bitdefender Wallet add-on is supported by the following browsers: Google Chrome, Internet Explorer and Mozilla Firefox, and is also also integrated with Safepay.

To access the Bitdefender Wallet extension, open your web browser, allow the add-on to be installed and click the icon on the toolbar.

The Bitdefender Wallet extension contains the following options:

- Open Wallet - opens the Wallet.
- Lock Wallet - locks the Wallet.
- Websites - opens a submenu with all the websites logins stored in the Wallet. Click **Add website** to add new websites into the list.
- Fill forms - opens a submenu containing the information you added for a specific category. From here you can add new data to your Wallet.
- Password Generator - enables you to generate random passwords you can use for new or existing accounts. Click **Show advanced settings** to customize the complexity of the password.

- Settings - opens the Password Manager settings window.
- Report issue - report any issue you encounter with the Bitdefender Password Manager.

27. PARENTAL ADVISOR

The Parental Advisor feature allows you to control the access to the Internet and to specific applications for each device the feature is installed on. Once you have configured Parental Advisor, you can easily find out what your child is doing on the devices he uses and where he has been in the last 24 hours. Moreover, to help you know better what your child is doing, the app gives you statistics about his activities and interests.

All you need is a computer with Internet access and a web browser.

You can configure Parental Advisor to block:

- inappropriate web pages.
- applications like games, chat, filesharing programs or others.
- block specific contacts that are not allowed to come in contact by phone with your child.

Check your children's activities and change the Parental Advisor settings using Bitdefender Central from any computer or mobile device connected to the Internet.

27.1. Accessing Parental Advisor - My Children

Once you access the Parental Advisor section, the **My Children** window is available. Here you can view and edit all the profiles you have created for your children. The profiles are displayed as profile cards, allowing you to quickly manage them and check their statuses at a glance.

As soon as you create a profile, you can start customizing more detailed settings to monitor and control the access to the Internet and to specific applications for your children.

You can access Parental Advisor settings from Bitdefender Central account on any computer or mobile device connected to the Internet.

Access your online account:

- On any device with Internet access:
  1. Access your Bitdefender Central account.

     Make sure that you are logged in with your credentials.
  2. Select the **Parental Advisor** panel.

3. In the **My Children** window that appears, you can manage and configure the Parental Advisor profiles for each device.

- From your Bitdefender interface:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Privacy** tab.
3. Under the **Parental Advisor** module, select **Configure**.

   You are redirected to the Bitdefender Central web page. Make sure that you are logged in with your credentials.
4. Select the **Parental Advisor** panel.
5. In the **My Children** window that appears, you can manage and configure the Parental Advisor profiles for each device.

Note
Make sure you are logged on to the computer with an administrator account. Only users with administrative rights on the system (system administrators) can access and configure Parental Advisor.

27.2. Adding your child's profile

To start monitoring your child's activities, you need to configure a profile and install the Bitdefender Parental Advisor Agent on devices he uses.

To add your child's profile to Parental Advisor:

1. Access the Parental Advisor panel from your Bitdefender Central account.
2. Click **ADD PROFILE** on the right-side of the **My Devices** window.
3. Set specific information in the corresponding fields, such as: name, e-mail, gender, and date of birth, and then click **CONTINUE**.

   Based on children development standards, setting the child's date of birth automatically loads specifications considered appropriate for his age category.
4. If your child's device already has Bitdefender Total Security 2016 installed, select his device from the available list, and then click **CONTINUE**.

   If your child's device has no Bitdefender product with the Parental Advisor feature included, click **Add a new device**. Select the operating system of his device, then click **CONTINUE**.

Type the e-mail address where we should send the installation download link of the Bitdefender Parental Advisor application.

On Windows based devices, the Bitdefender Total Security 2016 you have included in your subscription has to be downloaded and installed. On Android devices, the Bitdefender Parental Advisor Agent has to be downloaded and installed.

27.2.1. Linking Parental Advisor to Bitdefender Central

To monitor your child's online activity on Android, you must link his device to your Bitdefender Central account by logging in to the account from the app.

To link the device to your Bitdefender Central account, follow these steps:

1. Open the Parental Advisor app.
2. Check the **I declare that I'm the legal owner of the device** box and tap **Next**.
3. Log in to your existing Bitdefender Central account.

   If you do not have an account, choose to create a new account using the corresponding button.

   Note
   You may also enter a name for your device. If you link more than one device to your account, this will help you identify the devices more easily.

4. Tap **Link**.
5. Select the profile of the child you wish to monitor from the list and tap **Continue**.

   Alternatively, tap **Add new child** to create a new profile and fill in the required fields.
6. Activate device administrator rights for the app by tapping **Activate**.

   This will prevent your child from uninstalling the Parental Advisor Agent.

27.2.2. Monitoring the child's activity

Bitdefender helps you keep track of what your children are doing online.

In this way, you can always find out exactly what websites they have visited, what applications they have used or what activities have been blocked by the Parental Advisor.

Depending on the settings you make, the reports may contain detailed information for each event, such as:

- The status of the event.
- The notification severity.
- The device name.
- The date and time when the event occurred.

To monitor the Internet traffic, the accessed applications or the Facebook activity for your child, follow these steps:

1. Access the Parental Advisor panel from your Bitdefender Central account.
2. Select the desired device card.

   In the Timeline window you can view the information you are interested in.

27.2.3. Configuring the General Settings

By default, when Parental Advisor is enabled, your children's activities are logged.

To receive e-mail notifications, follow these steps:

1. Access the Parental Advisor panel from your Bitdefender Central account.
2. Click the icon on the top right corner.
3. Enable the corresponding option to receive activity reports.
4. Enter the e-mail address where the e-mail notifications are to be sent.
5. Adjust the frequency by selecting: weekly or monthly.
6. Receive e-mail notifications for the following:
   - Blocked websites
   - Blocked apps
   - Blocked IM contact
   - SMS from a blocked contact

- Call received from a blocked phone number
- Removal of Parental Advisor Facebook app

7. Click **Save**.

27.2.4. Editing a profile

To edit an existing profile:

1. Access your Bitdefender Central account.
2. Select the **Parental Advisor** panel.
3. Click the icon on the desired profile card, and then select **Edit**.
4. After customizing the desired settings, select **Save**.

27.2.5. Removing a profile

To remove an existing profile:

1. Access your Bitdefender Central account.
2. Select the **Parental Advisor** panel.
3. Click the icon on the desired profile card, and then select **Remove**.

27.3. Configuring Parental Advisor profiles

To start monitoring your child, a profile needs to be assigned to the device that has installed the Bitdefender Parental Advisor Agent.

After adding a profile for your child, you can customize more detailed settings to monitor and control the access to the Internet and to specific applications.

To start configuring a profile, select the desired profile card from the **My Children** window.

Click a tab to configure the corresponding Parental Advisor feature for the device:

- Timeline - displays all the activities, interests, locations, and interactions with friends, from the current day.
- Activities - allows you to block the access to certain applications, such as games, messaging software, movies, etc.

- Interests - allows you to filter web navigation and set time restrictions on Internet access.
- Friends - here you can specify which contacts from your child's list are allowed to come in contact with him by phone.
- Places - here you can set locations that are safe or not for your child.
- Social - allows you to block the access to social networks.

27.3.1. Timeline

The Timeline window gives you detailed information about your children's activities from the last 24 hours, inside and outside the home.

The Timeline window includes information about:

- **Locations** - here you can view the locations where your child was during the day. Click the **Set Sleep Time** link to set a time when the activities monitoring shall be automatically switched to the standby mode.
- **Interests** - here you can view info about what the categories of websites that your child visited. Click the **Review inappropriate content** link to have access to the inappropriate content that he watched.
- **Social Interactions** - here you can view a bar diagram with a top of the activities over the day.
- **Activities** - here you can view the contacts who called your child, the info he shared on Facebook and the new friends he added to his network.
- **Applications** - here you can see the applications your child used.

Note
For detailed information, click the desired option located in the right corner of every section.

27.3.2. Activities

The Activities window helps you block applications from running. Games, media and messaging software, as well as other categories of software can be blocked this way.

The module can be enabled or disabled by using the corresponding switch.

To configure Application control for a specific user account, follow these steps:

1. A list with cards is displayed. The cards represent the apps your child uses.
2. Select the card with the app you want your child to stop using.

   The check mark symbol that appears indicates that your child will not be able to use the app.

27.3.3. Interests

The Interests window helps you block websites with inappropriate content. Websites that host videos, games, media and messaging software, as well as other categories of negative content can be blocked this way.

The module can be enabled or disabled by using the corresponding switch.

Depending on the age you set for your child, the Interests list comes by default with a selection of categories enabled. To allow or deny the access to a specific category, click it.

The check mark symbol that appears indicates that your child will not be able to access content related to a specific category.

Allowing or blocking a website

To allow or restrict the access to certain web pages, you have to add them to the Exclusions list, as follows:

1. Click the **MANAGE** button.
2. Type the web page you want to allow or block in the corresponding field.
3. Select **Allow** or **Deny**.
4. Click **Done** to save the changes.

27.3.4. Friends

The Friends window gives you the possibility to specify which friends from your child's list are allowed or not to come in contact with him by phone.

To restrict a specific phone number of a friend, first you need to add the phone number of your child to his profile:

1. Select the **Parental Advisor** tab in your Bitdefender Central account.
2. Click the ⋮ icon on the desired profile card, and then select **Edit**.

3. Type in the corresponding field the phone number of your child, then click **SAVE**.
4. Select the profile of the child you want to set restrictions.
5. Select the **Friends** tab.

   A list with cards is displayed. The cards represent the contacts from your child's phone.
6. Select the card with the phone number you want block.

   The check mark symbol that appears indicates that your child will not be reached by the selected phone number.

To block unknown phone numbers, enable the **Block no caller ID interactions** switch.

27.3.5. Places

View the device's current location on Google Maps. The location is refreshed every 5 seconds, so you can track it if it is on the move.

The accuracy of the location depends on how Bitdefender is able to determine it:

- If the GPS is enabled on the device, its location can be pinpointed to within a couple of meters as long it is in the range of GPS satellites (i.e. not inside a building).
- If the device is indoors, its location can be determined to within tens of meters if Wi-Fi is enabled and there are wireless networks available in its range.
- Otherwise, the location will be determined using only information from the mobile network, which can offer an accuracy no better than several hundred meters.

To be sure that your child goes to certain locations, you can make a list of safe and unsafe places.

To configure a location:

1. Click **Devices** in the frame you have in the **Places** window.
2. Click **CHOOSE DEVICES**, and then select the device you want to configure.
3. In the **Areas** window, click the **ADD AREA** button.

4. Choose the type of the location, **Safe** or **Restricted**.
5. Type a valid name for the area where your child has permissions to go or not.
6. In the **Original Location**, type the town where your child should be located, and then choose the district from the list that appears.
7. Set the range that should be applied for monitoring from the **Radius** slide bar.
8. Click **ADD AREA** to save your settings.

27.3.6. Social

Parental Advisor monitors your child's Facebook account and reports the main activities taking place.

These online activities are verified and you are warned if they prove to be a threat for your child's privacy.

The monitored elements of the online account include:

- the number of friends
- comments of the child or his friends on his photos or posts
- messages
- wall posts
- uploaded photos and videos
- account privacy settings

To configure Facebook protection for a specific user account:

1. Type the e-mail of your monitored child account, and then click **SEND**.

   Inform your child about your intentions, and ask him to click the activation link he received from us in his e-mail.

2. To protect the child's Facebook account, he should click the **INSTALL APPLICATION** button that appears as soon as he access his Facebook account.

To stop monitoring the Facebook account, use the **Unlink account** button from the top.

28. DEVICE ANTI-THEFT

Laptop theft is a major issue that affects individuals and organizations alike. Even more than losing the hardware itself, the data lost with it can cause significant damage, both financially and emotionally.

Yet few people take the proper steps to secure their important personal, business and financial data in the case of theft or loss.

Bitdefender Anti-Theft helps you be better prepared for such an event by allowing you to remotely locate or lock your computer and even wipe all data from it, should you ever part with your computer against your will.

To use the Anti-Theft features, the following prerequisites must be met:

- The commands can only be sent from the Bitdefender Central account.
- The computer must be connected to the Internet to receive the commands.

Anti-Theft features work in the following way:

Locate

View your device's location on Google Maps.

The accuracy of the location depends on how Bitdefender is able to determine it. The location is determined to within tens of meters if Wi-fi is enabled on your computer and there are wireless networks in its range.

If the computer is connected to a wired LAN with no Wi-fi based location available, the location will be determined based on the IP address, which is considerably less accurate.

Alert

Send a remote alert on the device.

The feature is only available on mobile devices.

Lock

Lock your computer and set a 4 digit PIN for unlocking it. When you send the Lock command, the computer reboots and logging back into Windows is only possible after entering the PIN you have set.

Wipe

Remove all data from your computer. When you send the Wipe command, the computer reboots and the data on all hard drive partitions is erased.

Anti-Theft is activated after the installation and can be accessed exclusively through your Bitdefender Central account from any device connected to the Internet, anywhere.

Using Anti-Theft features

To access the Anti-Theft features, use one of the following possibilities:

- From the Bitdefender main interface:
  1. Click the icon in the lower-left corner of the Bitdefender interface.
  2. Select the **Tools** tab.
  3. Under the **Anti-Theft** module, select **Manage devices**.
  4. In the Bitdefender Central window that opens, click the desired device card, then select **Anti-Theft**.
- On any device with Internet access:
  1. Open a web browser and go to: https://central.bitdefender.com.
  2. Log in to your account using your e-mail address and password.
  3. Select the **My Devices** panel.
  4. Click the desired device card, then select **Anti-Theft**.
  5. Select the feature you want to use:

     Locate - display your device's location on Google Maps.

     Wipe - delete all data from your computer.

     Important
     After you wipe a device, all Anti-Theft features cease to function.

     Lock - lock your computer and set a PIN code for unlocking it.

     Alert - send an alert on the device.

29. USB IMMUNIZER

The Autorun feature built into Windows operating systems is a very useful tool that allows computers to automatically execute a file from media connected to it. For example, software installations can start automatically when a CD is inserted into the optical drive.

Unfortunately, this feature can also be used by malware to automatically launch and infiltrate your computer from rewritable media such as USB flash drives and memory cards connected through card readers. Numerous Autorun based attacks have been created in recent years.

With USB Immunizer you can prevent any NTFS, FAT32 or FAT formatted flash drive from automatically executing malware ever again. Once an USB device is immunized, malware can no longer configure it to run a certain application when the device is connected to a computer running Windows.

To immunize an USB device, follow these steps:

1. Connect the flash drive to your computer.
2. Browse your computer to locate the removable storage device and right-click its icon.
3. In the contextual menu, point to **Bitdefender** and select **Immunize this drive**.

Note
If the drive has already been immunized, the message **The USB device is protected against autorun-based malware** will appear instead of the Immunize option.

To prevent your computer from launching malware from unimmunized USB devices, disable the media autorun feature. For more information, please refer to "*Using automatic vulnerability monitoring*" (p. 124).

SYSTEM OPTIMIZATION

30. TUNE-UP

Bitdefender comes with a Tune-Up module that helps you maintain the integrity of your system. The maintenance tools offered are critical for the improvement of your system's responsiveness and the efficient management of the hard drive space.

Bitdefender provides the following PC tune-up tools:

- OneClick Optimizer analyzes and improves your system speed by running multiple tasks with a single click on a button.
- Startup Optimizer reduces your system startup time by stopping unnecessary applications from running when the PC is rebooted.

30.1. Optimizing your system speed with a single click

Issues such as hard disk failures, leftover registry files and browser history, may slow down your computer work, which may become nagging for you. All these can now be fixed with one single click on a button.

OneClick Optimizer allows you to identify and remove useless files, by running multiple cleaning tasks at the same time.

To start the OneClick Optimizer process, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Under the **Tune-Up** module, select **OneClick Optimizer**. To exit, click **Cancel**.
   a. **Analyzing**

      Wait for Bitdefender to finish searching for system issues.

      - Disk Cleanup - identifies old and useless system files.
      - Registry Cleanup - identifies invalid or outdated references in the Windows Registry.
      - Privacy Cleanup - identifies temporary Internet files and cookies, browser cache and history.

      The number of found issues is displayed. It is recommended to review them before proceeding with the cleaning process. Click **Optimize** to continue.

b. **System optimization**

Wait for Bitdefender to finish optimizing your system.

c. **Issues**

This is where you can view the operation result.

If you want comprehensive information on the optimization process, click the **View detailed report** link.

Or quicker, click the **OneClick Optimizer** action button from the Bitdefender interface.

30.2. Optimizing your PC's boot time

Extended system startup is a real problem due to applications that are set to run without being necessary. Waiting several minutes for a system to boot can cost you valuable time and productivity.

The Startup Optimizer window displays what applications are running during system startup and lets you manage their behavior at this step.

To start the Startup Optimizer process, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Under the **Tune-Up** module, select **Startup Optimizer**.

   a. **Select applications**

   You can see a list of the applications that are running at system startup. Select the ones you want to disable or delay at startup.

   b. **Community choice**

   See what other Bitdefender users have decided to do with the app you have selected.

   c. **System boot time**

   Check the slider at the top of the window to see the time required by both your system and the selected applications to run at startup.

   A system restart is required to be able to retrieve information about system and applications startup time.

   d. **Startup status**

- **Enable.** Select this option when you want an application to start running at system startup. This option is enabled by default.
- **Delay.**

  Select this option to postpone a program from running at system startup. This means that the selected applications will start with a five-minute delay after user logins on system.
  The **Delay** functionality is predefined and cannot be configured by user.
- **Disable.** Select this option to disable a program from running at system startup.

e. **Results**

Information such as the estimated system boot time after delaying or disabling programs is displayed.

A system restart may be required in order to see all this info.

Click **OK** to save the changes and close the window.

Or quicker, click the **Startup Optimizer** action button from the Bitdefender interface.

Note
In case your subscription expires or you decide to uninstall Bitdefender, the programs that you scheduled to stop running from startup will be restored to their default startup settings.

31. PROFILES

Daily job activities, watching movies or playing games may cause system slow down, especially if they are running simultaneously with Windows update processes and maintenance tasks. With Bitdefender, you can now choose and apply your preferred profile, which makes system adjustments suited to increase the performance of specific installed applications.

Bitdefender provides the following profiles:

- Work Profile
- Movie Profile
- Game Profile

If you decide to not use **Profiles**, a default profile called **Standard** is enabled and it brings no optimization to your system.

According to your activity, the following product settings are applied when a profile is activated:

- All Bitdefender alerts and pop-ups are disabled.
- Automatic Update is postponed.
- Scheduled scans are postponed.
- Search Advisor is disabled.
- Intrusion Detection is set to the **Permissive** protection level.
- Special offers and product notifications are disabled.

According to your activity, the following system settings are applied when a profile is activated:

- Windows Automatic Updates are postponed.
- Windows alerts and pop-ups are disabled.
- Unnecessary background programs are suspended.
- Visual effects are adjusted for best performance.
- Maintenance tasks are postponed.
- Power plan settings are adjusted.

31.1. Work Profile

Running multiple tasks at work, such as sending e-mails, having a video communication with your distant colleagues or working with design applications may affect your system performance. Work Profile has been designed to help you improve your work efficiency, by turning off some of your background services and maintenance tasks.

Configuring Work profile

To configure the actions to be taken while in Work Profile, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module.
4. In the **Profiles Settings** window, click the **Configure** button from the Work Profile area.
5. Choose the system adjustments you would like to be applied by checking the following options:
   - Boost performance on work apps
   - Optimize product settings for Work profile
   - Postpone background programs and maintenance tasks
   - Postpone Windows Automatic Updates
6. Click **Save** to save the changes and close the window.

Manually adding applications to the Work Profile list

If Bitdefender does not automatically enter Work Profile when you launch a certain work application, you can manually add the application to the **Applications list**.

To manually add applications to the Applications list in Work Profile:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.

3. Click the **Profiles** module, then click the **Configure** button from the Work profile area.
4. In the **Work profile** window, click the **Applications list** link.
5. Click **Add** to add a new application to the **Applications list**.

   A new window appears. Browse to the application's executable file, select it and click **OK** to add it to the list.

31.2. Movie Profile

Displaying high quality video content, such as high definition movies, requires significant system resources. Movie Profile adjusts system and product settings so you can enjoy an uninterrupted and seamless movie experience.

Configuring Movie Profile

To configure the actions to be taken while in Movie Profile:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module.
4. In the **Profiles Settings** window, click the **Configure** button from the Movie profile area.
5. Choose the system adjustments you would like to be applied by checking the following options:
   - Boost performance on video players
   - Optimize product settings for Movie profile
   - Postpone background programs and maintenance tasks
   - Postpone Windows Automatic Updates
   - Adjust power plan settings for movies
6. Click **Save** to save the changes and close the window.

Manually adding video players to the Movie Profile list

If Bitdefender does not automatically enter Movie Profile when you launch a certain video player application, you can manually add the application to the **Players list**.

To manually add video players to the Players list in Movie Profile:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module, then click the **Configure** button from the Movie Profile area.
4. In the **Movie Profile** window, click the **Players list** link.
5. Click **Add** to add a new application to the **Players list**.

   A new window appears. Browse to the application's executable file, select it and click **OK** to add it to the list.

31.3. Game Profile

Enjoying an uninterrupted gaming experience is all about reducing system interruption and diminishing slowdowns. By using behavioral heuristics along with a list of known games, Bitdefender can automatically detect running games and optimize your system resources so that you can enjoy your gaming break.

Configuring Game Profile

To configure the actions to be taken while in Game Profile, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module.
4. In the **Profiles Settings** window, click the **Configure** button from the Game Profile area.
5. Choose the system adjustments you would like to be applied by checking the following options:

- Boost performance on games
- Optimize product settings for Game profile
- Postpone background programs and maintenance tasks
- Postpone Windows Automatic Updates
- Adjust power plan settings for games

6. Click **Save** to save the changes and close the window.

Manually adding games to the Game list

If Bitdefender does not automatically enter Game Profile when you launch a certain game or application, you can manually add the application to the **Games list**.

To manually add games to the Games list in Game Profile:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.
3. Click the **Profiles** module, then click the **Configure** button from the Game Profile area.
4. In the **Game Profile** window, click the **Games list** link.
5. Click **Add** to add a new game to the **Games list**.

   A new window appears. Browse to the game's executable file, select it and click **OK** to add it to the list.

31.4. Real-Time Optimization

Bitdefender Real-Time Optimization is a plugin that improves your system performance silently, in the background, making sure that you are not interrupted while you are in a profile mode. Depending on the CPU load, the plugin monitors all processes, focusing on those that take up a higher load, to adjust them to your needs.

To turn on or off Real-Time Optimization, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Tools** tab.

3. Click the **Profiles** module, then select the **Profiles Settings** tab.
4. Turn on or off automatic Real-Time Optimization by clicking the corresponding switch.

TROUBLESHOOTING

32. SOLVING COMMON ISSUES

This chapter presents some problems you may encounter when using Bitdefender and provides you with possible solutions to these problems. Most of these problems can be solved through the appropriate configuration of the product settings.

- "*My system appears to be slow*" (p. 175)
- "*Scan doesn't start*" (p. 176)
- "*I can no longer use an application*" (p. 179)
- "*What to do when Bitdefender blocks a safe website or online application*" (p. 180)
- "*How to update Bitdefender on a slow Internet connection*" (p. 184)
- "*My computer is not connected to the Internet. How do I update Bitdefender?*" (p. 185)
- "*Bitdefender services are not responding*" (p. 185)
- "*Antispam filter does not work properly*" (p. 186)
- "*The Autofill feature in my Wallet doesn't work*" (p. 191)
- "*Bitdefender removal failed*" (p. 192)
- "*My system doesn't boot up after installing Bitdefender*" (p. 193)

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter "*Asking for help*" (p. 205).

32.1. My system appears to be slow

Usually, after installing a security software, there may appear a slight slowdown of the system, which to a certain degree is normal.

If you notice a significant slowdown, this issue can appear for the following reasons:

- **Bitdefender is not the only security program installed on the system.**

  Though Bitdefender searches and removes the security programs found during the installation, it is recommended to remove any other antivirus

program you may use before installing Bitdefender. For more information, please refer to "*How do I remove other security solutions?*" (p. 80).

- **The Minimum System Requirements for running Bitdefender are not met.**

  If your machine does not meet the Minimum System Requirements, the computer will become sluggish, especially when multiple applications are running at the same time. For more information, please refer to "*Minimum system requirements*" (p. 3).

- **You have installed applications that you do not use**.

  Any computer has programs or applications that you do not use. And many unwanted programs run in the background taking up disk space and memory. If you do not use a program, uninstall it. This is also valid for any other pre-installed software or trial application you forgot to remove.

  > **Important**
  > If you suspect a program or an application to be an essential part of your operating system, do not remove it and contact Bitdefender Customer Care for assistance.

- **Your system may be infected**.

  Your system speed and its general behavior can also be affected by malware. Spyware, viruses, Trojans and adware all take a toll on your computer's performance. Make sure to scan your system periodically, at least once a week. It is recommended to use the Bitdefender System Scan because it scans for all types of malware threatening the security of your system.

  To start the System Scan, follow these steps:

  1. Click the icon in the lower-left corner of the Bitdefender interface.
  2. Select the **Protection** tab.
  3. Under the **Antivirus** module, select **System Scan**.
  4. Follow the wizard steps.

32.2. Scan doesn't start

This type of issue can have two main causes:

- **A previous Bitdefender installation which was not completely removed or a faulty Bitdefender installation**.

  In this case, follow these steps:

  1. Remove Bitdefender completely from the system:
     - In **Windows 7**:
       a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
       b. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       c. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       d. Click **Next** to continue.
       e. Wait for the uninstall process to complete, then reboot your system.
     - In **Windows 8 and Windows 8.1**:
       a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
       b. Click **Uninstall a program** or **Programs and Features**.
       c. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       d. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       e. Click **Next** to continue.
       f. Wait for the uninstall process to complete, then reboot your system.
     - In **Windows 10**:
       a. Click **Start**, then click Settings.
       b. Click the **System** icon in the Settings area, then select **Installed apps**.
       c. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       d. Click **Uninstall** again to confirm your choice.
       e. Click **Remove** in the window that appears, and then select **I want to reinstall it**.

f. Click **Next** to continue.

g. Wait for the uninstall process to complete, then reboot your system.

2. Reinstall your Bitdefender product.

- **Bitdefender is not the only security solution installed on your system**.

  In this case, follow these steps:

  1. Remove the other security solution. For more information, please refer to "*How do I remove other security solutions?*" (p. 80).
  2. Remove Bitdefender completely from the system:
     - In **Windows 7**:
       a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
       b. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       c. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       d. Click **Next** to continue.
       e. Wait for the uninstall process to complete, then reboot your system.
     - In **Windows 8 and Windows 8.1**:
       a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
       b. Click **Uninstall a program** or **Programs and Features**.
       c. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       d. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       e. Click **Next** to continue.
       f. Wait for the uninstall process to complete, then reboot your system.
     - In **Windows 10**:
       a. Click **Start**, then click Settings.
       b. Click the **System** icon in the Settings area, then select **Installed apps**.

c. Find **Bitdefender Total Security 2016** and select **Uninstall**.

d. Click **Uninstall** again to confirm your choice.

e. Click **Remove** in the window that appears, and then select **I want to reinstall it**.

f. Click **Next** to continue.

g. Wait for the uninstall process to complete, then reboot your system.

3. Reinstall your Bitdefender product.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.3. I can no longer use an application

This issue occurs when you are trying to use a program which was working normally before installing Bitdefender.

After installing Bitdefender you may encounter one of these situations:

- You could receive a message from Bitdefender that the program is trying to make a modification to the system.
- You could receive an error message from the program you're trying to use.

This type of situation occurs when Active Threat Control mistakenly detects some applications as malicious.

Active Threat Control is a Bitdefender module which constantly monitors the applications running on your system and reports those with potentially malicious behavior. Since this feature is based on a heuristic system, there may be cases when legitimate applications are reported by Active Threat Control.

When this situation occurs, you can exclude the respective application from being monitored by Active Threat Control.

To add the program to the exclusions list, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Antivirus** module, then select the **Exclusions** tab.

4. Click the **Excluded Processes** link. In the window that appears, you can manage the Active Threat Control process exclusions.
5. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
   c. Keep the **Allow** option selected to prevent Active Threat Control from blocking the application.
   d. Click **Add**.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.4. What to do when Bitdefender blocks a safe website or online application

Bitdefender offers a secure web browsing experience by filtering all web traffic and blocking any malicious content. However, it is possible that Bitdefender considers a safe website or online application as unsafe, which will cause Bitdefender HTTP traffic scanning to block them incorrectly.

Should the same page or application be blocked repeatedly, they can be added to a whitelist so that they will not be scanned by the Bitdefender engines, thus ensuring a smooth web browsing experience.

To add a website to the **Whitelist**, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Web Protection** module.
4. In the **Settings** tab, click the **Whitelist** link.
5. Provide the address of the blocked website or online application in the corresponding field and click **Add**.
6. Click **Save** to save the changes and close the window.

Only websites and applications that you fully trust should be added to this list. These will be excluded from scanning by the following engines: malware, phishing and fraud.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.5. I cannot connect to the Internet

You may notice that a program or a web browser can no longer connect to the Internet or access network services after installing Bitdefender.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective software application:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Click the **Firewall** module, then select the **Rules** tab.
4. To add an application rule, click the **Add rule** button.
5. A new window appears where you can add the details. Make sure to select all the network types available and in the **Permission** section select **Allow**.

Close Bitdefender, open the software application and try again to connect to the Internet.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.6. I cannot access a device on my network

Depending on the network you are connected to, the Bitdefender firewall may block the connection between your system and another device (such as another computer or a printer). As a result, you may no longer share or print files.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective device. For each network connection you can configure a special trusted zone.

A trusted zone is a device that you fully trust. All traffic between your computer and the trusted device is allowed. To share resources with specific devices, such as computers or printers, add them as trusted zones.

To add a trusted zone on your network adapters, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Click the **Firewall** module, then select the **Rules** tab.
4. To add a zone, click the **Add rule** button. A new window displaying the IP addresses of the devices connected to the network will appear.
5. Select the IP address of the computer or the printer you want to add, or type an address or address range in the provided text box.
6. In the **Permission** field select **Allow** and then click **OK**.

If you still cannot connect to the device, the issue may not be caused by Bitdefender.

Check for other potential causes, such as the following:

- The firewall on the other computer may block file and printer sharing with your computer.
  - If the Windows Firewall is used, it can be configured to allow file and printer sharing as follows:
    - In **Windows 7**:
      1. Click **Start**, go to **Control Panel** and select **System and Security**.
      2. Go to **Windows Firewall** and click **Allow a program through Windows Firewall**.
      3. Select **File and Printer Sharing** check box.
    - In **Windows 8 and Windows 8.1**:
      1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
      2. Click **System and Security**, go to **Windows Firewall** and select **Allow an app through Windows Firewall**.
      3. Select **File and Printer Sharing** check box and click **OK**.
    - In **Windows 10**:
      1. Type "Allow an app through Windows Firewall" in the search box from the taskbar and click its icon.
      2. Click **Change settings**.

3. In the **Allowed apps and features** list select the **File and Printer Sharing** check box and click **OK**.

- If another firewall program is used, please refer to its documentation or help file.

- General conditions that may prevent using or connecting to the shared printer:
  - You may need to log on to a Windows administrator account to access the shared printer.
  - Permissions are set for the shared printer to allow access to specific computer and users only. If you are sharing your printer, check the permissions set for the printer to see if the user on the other computer is allowed access to the printer. If you are trying to connect to a shared printer, check with the user on the other computer if you have permission to connect to the printer.
  - The printer connected to your computer or to the other computer is not shared.
  - The shared printer is not added on the computer.

  Note
  To learn how to manage printer sharing (share a printer, set or remove permissions for a printer, connect to a network printer or to a shared printer), go to the Windows Help and Support Center (in the Start menu, click **Help and Support**).

- Access to a network printer may be restricted to specific computers or users only. You should check with the network administrator if you have permission to connect to that printer.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.7. My Internet is slow

This situation may appear after you install Bitdefender. The issue could be caused by errors in the Bitdefender firewall configuration.

To troubleshoot this situation, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Click the **Firewall** module, then click the switch to turn off **Firewall**.
4. Check if your Internet connection improved with the Bitdefender firewall disabled.
   - If you still have a slow Internet connection, the issue may not be caused by Bitdefender. You should contact your Internet Service Provider to verify if the connection is operational on their side.

     If you receive confirmation from your Internet Service Provider that the connection is operational on their side and the issue still persists, contact Bitdefender as described in section "*Asking for help*" (p. 205).
   - If the Internet connection improved after disabling the Bitdefender firewall, follow these steps:
     a. Click the icon in the lower-left corner of the Bitdefender interface.
     b. Select the **Protection** tab.
     c. Click the **Firewall** module, then select the **Settings** tab.
     d. Go to **Block port scans in the network** and click the switch to turn it off.
     e. Go to the **Adapters** tab and select your Internet connection.
     f. In the **Network Type** column and select **Home/Office**.
     g. In the **Stealth Mode** column select **ON**. Set the **Generic** column to **On**.
     h. Close Bitdefender, reboot the system and check the Internet connection speed.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.8. How to update Bitdefender on a slow Internet connection

If you have a slow Internet connection (such as dial-up), errors may occur during the update process.

To keep your system up to date with the latest Bitdefender malware signatures, follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **General Settings** from the drop-down menu.
2. In the **General Settings** window, select the **Update** tab.
3. Next to **Update processing rules**, select **Prompt before downloading** from the drop-down menu.
4. Go back to the main window and click the **Update** action button from the Bitdefender interface.
5. Select only **Signatures updates** and then click **OK**.
6. Bitdefender will download and install only the malware signature updates.

32.9. My computer is not connected to the Internet. How do I update Bitdefender?

If your computer is not connected to the Internet, you must download the updates manually to a computer with Internet access and then transfer them to your computer using a removable device, such as a flash drive.

Follow these steps:

1. On a computer with Internet access, open a web browser and go to:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. In the **Manual Update** column, click the link corresponding to your product and system architecture. If you do not know whether your Windows is running on 32 or 64 bits, please refer to *"Am I using a 32 bit or a 64 bit version of Windows?" (p. 78)*.
3. Save the file named weekly.exe to the system.
4. Transfer the downloaded file on a removable device, such as a flash drive, and then to your computer.
5. Double-click the file and follow the wizard steps.

32.10. Bitdefender services are not responding

This article helps you troubleshoot the **Bitdefender Services are not responding** error. You may encounter this error as follows:

- The Bitdefender icon in the system tray is grayed out and you are informed that the Bitdefender services are not responding.

- The Bitdefender window indicates that the Bitdefender services are not responding.

The error may be caused by one of the following conditions:

- temporary communication errors between the Bitdefender services.
- some of the Bitdefender services are stopped.
- other security solutions running on your computer at the same time with Bitdefender.

To troubleshoot this error, try these solutions:

1. Wait a few moments and see if anything changes. The error may be temporary.
2. Restart the computer and wait a few moments until Bitdefender is loaded. Open Bitdefender to see if the error persists. Restarting the computer usually solves the problem.
3. Check if you have any other security solution installed as they may disrupt the normal operation of Bitdefender. If this is the case, we recommend you to remove all of the other security solutions and then reinstall Bitdefender.

   For more information, please refer to "*How do I remove other security solutions?*" (p. 80).

If the error persists, please contact our support representatives for help as described in section "*Asking for help*" (p. 205).

32.11. Antispam filter does not work properly

This article helps you troubleshoot the following problems concerning the Bitdefender Antispam filtering operation:

- A number of legitimate e-mail messages are marked as [spam].
- Many spam messages are not marked accordingly by the antispam filter.
- The antispam filter does not detect any spam message.

32.11.1. Legitimate messages are marked as [spam]

Legitimate messages are marked as [spam] simply because they look like spam to the Bitdefender antispam filter. You can normally solve this problem by adequately configuring the Antispam filter.

Bitdefender automatically adds the receivers of your e-mail messages to a Friends List. The e-mail messages received from the contacts in the Friends list are considered to be legitimate. They are not verified by the antispam filter and, thus, they are never marked as [spam].

The automatic configuration of the Friends list does not prevent the detection errors that may occur in these situations:

- You receive a lot of solicited commercial mail as a result of subscribing on various websites. In this case, the solution is to add the e-mail addresses from which you receive such e-mail messages to the Friends list.
- A significant part of your legitimate mail is from people to whom you never e-mailed before, such as customers, potential business partners and others. Other solutions are required in this case.

  If you are using one of the mail clients Bitdefender integrates into, indicate detection errors.

> **Note**
> Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 108).

Add contacts to Friends List

If you are using a supported mail client, you can easily add the senders of legitimate messages to the Friends list. Follow these steps:

1. In your mail client, select an e-mail message from the sender that you want to add to the Friends list.
2. Click the **Add Friend** button on the Bitdefender antispam toolbar.
3. You may be asked to acknowledge the addresses added to the Friends list. Select **Don't show this message again** and click **OK**.

You will always receive e-mail messages from this address no matter what they contain.

If you are using a different mail client, you can add contacts to the Friends list from the Bitdefender interface. Follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Under the **Antispam** module, select **Manage Friends**.

   A configuration window appears.
4. Type the e-mail address you always want to receive e-mail messages from and then click **Add**. You can add as many e-mail addresses as you want.
5. Click **OK** to save the changes and close the window.

Indicate detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as [spam]). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the legitimate message incorrectly marked as [spam] by Bitdefender.
4. Click the **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
5. Click the **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The e-mail message will be moved to the Inbox folder.

32.11.2. Many spam messages are not detected

If you are receiving many spam messages that are not marked as [spam], you must configure the Bitdefender antispam filter so as to improve its efficiency.

Try the following solutions:

1. If you are using one of the mail clients Bitdefender integrates into, indicate undetected spam messages.

Note

Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 108).

2. Add spammers to the Spammers list. The e-mail messages received from addresses in the Spammers list are automatically marked as [spam].

Indicate undetected spam messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

Add spammers to Spammers List

If you are using a supported mail client, you can easily add the senders of the spam messages to the Spammers list. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the messages marked as [spam] by Bitdefender.
4. Click the **Add Spammer** button on the Bitdefender antispam toolbar.
5. You may be asked to acknowledge the addresses added to the Spammers list. Select **Don't show this message again** and click **OK**.

If you are using a different mail client, you can manually add spammers to the Spammers list from the Bitdefender interface. It is convenient to do this only when you have received several spam messages from the same e-mail address. Follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.

2. Select the **Protection** tab.
3. Under the **Antispam** module, select **Manage Spammers**.

   A configuration window appears.
4. Type the spammer's e-mail address and then click the **Add**. You can add as many e-mail addresses as you want.
5. Click **OK** to save the changes and close the window.

32.11.3. Antispam filter does not detect any spam message

If no spam message is marked as [spam], there may be a problem with the Bitdefender Antispam filter. Before troubleshooting this problem, make sure it is not caused by one of the following conditions:

- Antispam protection might be turned off. To verify the antispam protection status, click the arrow in the lower-left corner of the Bitdefender interface, select the **Protection** tab, click the **Antispam** module and check the switch in the **Settings** window.

  If Antispam is turned off, this is what is causing your problem. Click the switch to turn on your antispam protection.
- The Bitdefender Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. This means the following:
  - E-mail messages received via web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) are not filtered for spam by Bitdefender.
  - If your e-mail client is configured to receive e-mail messages using other protocol than POP3 (for example, IMAP4), the Bitdefender Antispam filter does not check them for spam.

  Note

  POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server. If you do not know the protocol that your e-mail client uses to download e-mail messages, ask the person who configured your e-mail client.

- Bitdefender Total Security 2016 doesn't scan Lotus Notes POP3 traffic.

A possible solution is to repair or reinstall the product. However, you may want to contact Bitdefender for support instead, as described in section "*Asking for help*" (p. 205).

32.12. The Autofill feature in my Wallet doesn't work

You have saved your online credentials in your Bitdefender Wallet and you noticed that the autofill is not working. Usually, this issue appears when the Bitdefender Password Manager extension is not installed in your browser.

To fix this situation, follow these steps:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Click Tools.
  3. Click Manage add-ons.
  4. Click Toolbars and Extensions.
  5. Point **Bitdefender Password Manager** and click Enable.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Click Tools.
  3. Click Add-ons.
  4. Click Extensions.
  5. Point **Bitdefender Password Manager** and click Enable.
- In **Google Chrome:**
  1. Open Google Chrome.
  2. Go to the Menu icon.
  3. Click Settings.
  4. Click Extensions.
  5. Point **Bitdefender Password Manager** and click Enable.

Note
The add-on will be enabled after you restart your web browser.

Now check if the autofill feature in Wallet works for your online accounts.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

32.13. Bitdefender removal failed

If you want to remove your Bitdefender product and you notice that the process hangs out or the system freezes, click **Cancel** to abort the action. If this does not work, restart the system.

When removal fails, some Bitdefender registry keys and files may remain in your system. Such remainders may prevent a new installation of Bitdefender. They may also affect system performance and stability.

In order to completely remove Bitdefender from your system, follow these steps:

- In **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  3. Select **Remove**, and then select **I want to permanently remove it**.
  4. Click **Next** to continue.
  5. Wait for the uninstall process to complete, then reboot your system.
- In **Windows 8 and Windows 8.1**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
  4. Select **Remove**, and then select **I want to permanently remove it**.
  5. Click **Next** to continue.
  6. Wait for the uninstall process to complete, then reboot your system.
- In **Windows 10**:
  1. Click **Start**, then click Settings.
  2. Click the **System** icon in the Settings area, then select **Installed apps**.

3. Find **Bitdefender Total Security 2016** and select **Uninstall**.
4. Click **Uninstall** again to confirm your choice.
5. Select **Remove**, and then select **I want to permanently remove it**.
6. Click **Next** to continue.
7. Wait for the uninstall process to complete, then reboot your system.

32.14. My system doesn't boot up after installing Bitdefender

If you just installed Bitdefender and cannot reboot your system in normal mode anymore there may be various reasons for this issue.

Most probably this is caused by a previous Bitdefender installation which was not removed properly or by another security solution still present on the system.

This is how you may address each situation:

- **You had Bitdefender before and you did not remove it properly.**

  To solve this, follow these steps:

  1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 81).
  2. Remove Bitdefender from your system:
     - In **Windows 7**:
       a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
       b. Find **Bitdefender Total Security 2016** and select **Uninstall**.
       c. Click **Remove** in the window that appears, and then select **I want to reinstall it**.
       d. Click **Next** to continue.
       e. Wait for the uninstall process to complete.
       f. Reboot your system in normal mode.
     - In **Windows 8 and Windows 8.1**:

a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.

b. Click **Uninstall a program** or **Programs and Features**.

c. Find **Bitdefender Total Security 2016** and select **Uninstall**.

d. Click **Remove** in the window that appears, and then select **I want to reinstall it**.

e. Click **Next** to continue.

f. Wait for the uninstall process to complete.

g. Reboot your system in normal mode.

- In **Windows 10**:

a. Click **Start**, then click Settings.

b. Click the **System** icon in the Settings area, then select **Installed apps**.

c. Find **Bitdefender Total Security 2016** and select **Uninstall**.

d. Click **Uninstall** again to confirm your choice.

e. Click **Remove** in the window that appears, and then select **I want to reinstall it**.

f. Click **Next** to continue.

g. Wait for the uninstall process to complete.

h. Reboot your system in normal mode.

3. Reinstall your Bitdefender product.

- **You had a different security solution before and you did not remove it properly.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 81).
2. Remove the other security solution from your system:

- In **Windows 7**:

a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.

b. Find the name of the program you want to remove and select **Remove**.

c. Wait for the uninstall process to complete, then reboot your system.

- In **Windows 8 and Windows 8.1**:

a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.

b. Click **Uninstall a program** or **Programs and Features**.

c. Find the name of the program you want to remove and select **Remove**.

d. Wait for the uninstall process to complete, then reboot your system.

- In **Windows 10**:

a. Click **Start**, then click Settings.

b. Click the **System** icon in the Settings area, then select **Installed apps**.

c. Find the name of the program you want to remove and select **Uninstall**.

d. Wait for the uninstall process to complete, then reboot your system.

In order to correctly uninstall the other software, go to their website and run their uninstall tool or contact them directly in order to provide you with the uninstall guidelines.

3. Reboot your system in normal mode and reinstall Bitdefender.

You have already followed the steps above and the situation is not solved.

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 81).
2. Use the System Restore option from Windows to restore the computer to an earlier date before installing the Bitdefender product.
3. Reboot the system in normal mode and contact our support representatives for help as described in section "*Asking for help*" (p. 205).

33. REMOVING MALWARE FROM YOUR SYSTEM

Malware can affect your system in many different ways and the Bitdefender approach depends on the type of malware attack. Because viruses change their behavior frequently, it is difficult to establish a pattern for their behavior and their actions.

There are situations when Bitdefender cannot automatically remove the malware infection from your system. In such cases, your intervention is required.

- "*Bitdefender Rescue Mode*" (p. 196)
- "*What to do when Bitdefender finds viruses on your computer?*" (p. 198)
- "*How do I clean a virus in an archive?*" (p. 199)
- "*How do I clean a virus in an e-mail archive? "* (p. 200)
- "*What to do if I suspect a file as being dangerous?*" (p. 201)
- "*What are the password-protected files in the scan log?*" (p. 202)
- "*What are the skipped items in the scan log?*" (p. 202)
- "*What are the over-compressed files in the scan log?*" (p. 203)
- "*Why did Bitdefender automatically delete an infected file?*" (p. 203)

If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter "*Asking for help*" (p. 205).

33.1. Bitdefender Rescue Mode

Rescue Mode is a Bitdefender feature that allows you to scan and disinfect all existing hard drive partitions outside of your operating system.

Once Bitdefender Total Security 2016 is installed, Rescue Mode can be used even if you are no longer able to boot into Windows.

Starting your system in Rescue Mode

You can enter Rescue Mode in one of two ways:

From the Bitdefender interface

To enter Rescue Mode directly from Bitdefender, follow these steps:

1. Click the icon in the lower-left corner of the Bitdefender interface.
2. Select the **Protection** tab.
3. Under the **Antivirus** module, select **Rescue Mode**.

   A confirmation window appears. Click **Yes** to reboot your computer.
4. After the computer restarts, a menu will appear prompting you to select an operating system. Choose **Bitdefender Rescue Mode** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
5. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

   Bitdefender Rescue Mode will load in a few moments.

Boot your computer directly into Rescue Mode

If Windows no longer starts, you can boot your computer directly into Bitdefender Rescue Mode by following the steps below:

1. Start / reboot your computer and start pressing the **space** key on your keyboard before the Windows logo appears.
2. A menu will appear prompting you to select an operating system to start. Press **TAB** to go to the tools area. Choose **Bitdefender Rescue Image** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
3. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

   Bitdefender Rescue Mode will load in a few moments.

Scanning your system in Rescue Mode

To scan your system in Rescue Mode, follow these steps:

1. Enter Rescue Mode, as described in “Starting your system in Rescue Mode” (p. 196).
2. The Bitdefender logo will appear and the antivirus engines will start to be copied.
3. A welcome window will then appear. Click **Continue**.
4. An update of the antivirus signatures is started.

5. After the update is completed, the Bitdefender On-demand Antivirus Scanner window appears.
6. Click **Scan Now**, select the scan target in the window that appears and click **Open** to start scanning.

   It is recommended to scan your entire Windows partition.

   Note
   When working in Rescue Mode, you are dealing with Linux-type partition names. Disk partitions will appear as sda1 probably corresponding to the (C:) Windows-type partition, sda2 corresponding to (D:) and so on.

7. Wait for the scan to complete. If any malware is detected, follow the instructions to remove the threat.
8. To exit Rescue Mode, right-click in an empty area of the desktop, select **Exit** in the menu that appears and then choose whether to reboot or shut down the computer.

33.2. What to do when Bitdefender finds viruses on your computer?

You may find out there is a virus on your computer in one of these ways:

- You scanned your computer and Bitdefender found infected items on it.
- A virus alert informs you that Bitdefender blocked one or multiple viruses on your computer.

In such situations, update Bitdefender to make sure you have the latest malware signatures and run a System Scan to analyze the system.

As soon as the system scan is over, select the desired action for the infected items (Disinfect, Delete, Move to quarantine).

Warning
If you suspect the file is part of the Windows operating system or that it is not an infected file, do not follow these steps and contact Bitdefender Customer Care as soon as possible.

If the selected action could not be taken and the scan log reveals an infection which could not be deleted, you have to remove the file(s) manually:

The first method can be used in normal mode:

1. Turn off the Bitdefender real-time antivirus protection:
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Protection** tab.
   c. Click the **Antivirus** module, then select the **Shield** tab.
   d. Click the switch to turn off **On-access scanning**.
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 79).
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Turn on the Bitdefender real-time antivirus protection.

In case the first method failed to remove the infection, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 81).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 79).
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

33.3. How do I clean a virus in an archive?

An archive is a file or a collection of files compressed under a special format to reduce the space on disk necessary for storing the files.

Some of these formats are open formats, thus providing Bitdefender the option to scan inside them and then take appropriate actions to remove them.

Other archive formats are partially or fully closed, and Bitdefender can only detect the presence of viruses inside them, but is not able to take any other actions.

If Bitdefender notifies you that a virus has been detected inside an archive and no action is available, it means that removing the virus is not possible due to restrictions on the archive's permission settings.

Here is how you can clean a virus stored in an archive:

1. Identify the archive that includes the virus by performing a System Scan of the system.
2. Turn off the Bitdefender real-time antivirus protection:
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Protection** tab.
   c. Click the **Antivirus** module, then select the **Shield** tab.
   d. Click the switch to turn off **On-access scanning**.
3. Go to the location of the archive and decompress it using an archiving application, like WinZip.
4. Identify the infected file and delete it.
5. Delete the original archive in order to make sure the infection is totally removed.
6. Recompress the files in a new archive using an archiving application, like WinZip.
7. Turn on the Bitdefender real-time antivirus protection and run a Full system scan in order to make sure there is no other infection on the system.

Note
It's important to note that a virus stored in an archive is not an immediate threat to your system, since the virus has to be decompressed and executed in order to infect your system.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

33.4. How do I clean a virus in an e-mail archive?

Bitdefender can also identify viruses in e-mail databases and e-mail archives stored on disk.

Sometimes it is necessary to identify the infected message using the information provided in the scan report, and delete it manually.

Here is how you can clean a virus stored in an e-mail archive:

1. Scan the e-mail database with Bitdefender.
2. Turn off the Bitdefender real-time antivirus protection:
   a. Click the icon in the lower-left corner of the Bitdefender interface.
   b. Select the **Protection** tab.
   c. Click the **Antivirus** module, then select the **Shield** tab.
   d. Click the switch to turn off **On-access scanning**.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the e-mail client.
4. Delete the infected messages. Most e-mail clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.
5. Compact the folder storing the infected message.
   - In Outlook Express: On the File menu, click Folder, then Compact All Folders.
   - In Microsoft Outlook 2007: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.
   - In Microsoft Outlook 2010 / 2013: On the File menu, click Info and then Account settings (Add and remove accounts or change existing connection settings). Then click Data File, select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.
6. Turn on the Bitdefender real-time antivirus protection.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 205).

33.5. What to do if I suspect a file as being dangerous?

You may suspect a file from your system as being dangerous, even though your Bitdefender product did not detect it.

To make sure your system is protected, follow these steps:

1. Run a **System Scan** with Bitdefender. To find out how to do this, please refer to "*How do I scan my system?*" (p. 58).
2. If the scan result appears to be clean, but you still have doubts and want to make sure about the file, contact our support representatives so that we may help you.

   To find out how to do this, please refer to "*Asking for help*" (p. 205).

33.6. What are the password-protected files in the scan log?

This is only a notification which indicates that Bitdefender has detected these files are either protected with a password or by some form of encryption.

Most commonly, the password-protected items are:

- Files that belong to another security solution.
- Files that belong to the operating system.

In order to actually scan the contents, these files would need to either be extracted or otherwise decrypted.

Should those contents be extracted, Bitdefender's real-time scanner would automatically scan them to keep your computer protected. If you want to scan those files with Bitdefender, you have to contact the product manufacturer in order to provide you with more details on those files.

Our recommendation to you is to ignore those files because they are not a threat for your system.

33.7. What are the skipped items in the scan log?

All files that appear as Skipped in the scan report are clean.

For increased performance, Bitdefender does not scan files that have not changed since the last scan.

33.8. What are the over-compressed files in the scan log?

The over-compressed items are elements which could not be extracted by the scanning engine or elements for which the decryption time would have taken too long making the system unstable.

Overcompressed means that Bitdefender skipped scanning within that archive because unpacking it proved to take up too many system resources. The content will be scanned on real time access if needed.

33.9. Why did Bitdefender automatically delete an infected file?

If an infected file is detected, Bitdefender will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

This is usually the case with installation files that are downloaded from untrustworthy websites. If you find yourself in such a situation, download the installation file from the manufacturer's website or other trusted website.

CONTACT US

34. ASKING FOR HELP

Bitdefender provides its customers with an unparalleled level of fast and accurate support. If you experience any issue or if you have any question about your Bitdefender product, you can use several online resources to find a solution or an answer. At the same time, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and will provide you with the assistance you need.

The "*Solving common issues*" (p. 175) section provides the necessary information regarding the most frequent issues you may encounter when using this product.

If you do not find an answer to your question in the provided resources, you can contact us directly:

- "Contact us directly from your Bitdefender product" (p. 205)
- "Contact us through our online Support Center" (p. 206)

Contact us directly from your Bitdefender product

If you have a working Internet connection, you can contact Bitdefender for assistance directly from the product interface.

Follow these steps:

1. Click the icon at the top of the Bitdefender interface and select **Help & Support** from the drop-down menu.
2. You have the following options:
   - **Product Documentation**

     Access our database and search for the necessary information.
   - **Contact Support**

     Use the **Contact Support** button to launch the Bitdefender Support Tool and contact the Customer Care Department. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

     a. Select the agreement check box and click **Next**.

     b. Complete the submission form with the necessary data:

        i. Enter your e-mail address.

ii. Enter your full name.

iii. Enter a description of the issue you encountered.

iv. Check the **Try to reproduce the issue before submitting** option in case you are encountering a product issue. Continue with the required steps.

c. Please wait for a few minutes while Bitdefender gathers product related information. This information will help our engineers find a solution to your problem.

d. Click **Finish** to send the information to the Bitdefender Customer Care Department. You will be contacted as soon as possible.

Contact us through our online Support Center

If you cannot access the necessary information using the Bitdefender product, please refer to our online Support Center:

1. Go to http://www.bitdefender.com/support/consumer.html.

   The Bitdefender Support Center hosts numerous articles that contain solutions to Bitdefender-related issues.

2. Use the search bar at the top of the window to find articles that may provide a solution to your problem. To search, just type a term in the Search bar and click **Search**.

3. Read the relevant articles or documents and try the proposed solutions.

4. If the solution does not solve your problem, go to

   http://www.bitdefender.com/support/contact-us.html and contact our support representatives.

35. ONLINE RESOURCES

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center:

  http://www.bitdefender.com/support/consumer.html

- Bitdefender Support Forum:

  http://forum.bitdefender.com

- The HOTforSecurity computer security portal:

  http://www.hotforsecurity.com

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

35.1. Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Support Center is available any time at

http://www.bitdefender.com/support/consumer.html.

35.2. Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others.

If your Bitdefender product does not operate well, if it cannot remove specific viruses from your computer or if you have questions about the way it works, post your problem or question on the forum.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Home & Home Office Protection** link to access the section dedicated to consumer products.

35.3. HOTforSecurity Portal

HOTforSecurity is a rich source of computer security information. Here you can learn about the various threats your computer is exposed to when connected to the Internet (malware, phishing, spam, cyber-criminals).

New articles are posted regularly to keep you up-to-date with the latest threats discovered, the current security trends and other information on the computer security industry.

The HOTforSecurity web page is http://www.hotforsecurity.com.

36. CONTACT INFORMATION

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

36.1. Web addresses

Sales department: sales@bitdefender.com
Support Center: http://www.bitdefender.com/support/consumer.html
Documentation: documentation@bitdefender.com
Local distributors: http://www.bitdefender.com/partners
Partner program: partners@bitdefender.com
Media relations: pr@bitdefender.com
Careers: jobs@bitdefender.com
Virus submissions: virus_submission@bitdefender.com
Spam submissions: spam_submission@bitdefender.com
Report abuse: abuse@bitdefender.com
Web site: http://www.bitdefender.com

36.2. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to http://www.bitdefender.com/partners/partner-locator.html.
2. Choose your country and city using the corresponding options.
3. If you do not find a Bitdefender distributor in your country, feel free to contact us by e-mail at sales@bitdefender.com. Please write your e-mail in English in order for us to be able to assist you promptly.

36.3. Bitdefender offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Phone (office&sales): 1-954-776-6262
Sales: sales@bitdefender.com
Technical support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

Germany

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Office: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Sales: vertrieb@bitdefender.de
Technical support: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Spain

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Phone: +34 902 19 07 65
Sales: comercial@bitdefender.es
Technical support: http://www.bitdefender.es/support/consumer.html
Website: http://www.bitdefender.es

Romania

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Sales phone: +40 21 2063470
Sales e-mail: sales@bitdefender.ro

Technical support: http://www.bitdefender.ro/support/consumer.html
Website: http://www.bitdefender.ro

United Arab Emirates

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Sales phone: 00971-4-4588935 / 00971-4-4589186
Sales e-mail: mena-sales@bitdefender.com
Technical support: http://www.bitdefender.com/support/consumer.html
Website: http://www.bitdefender.com

Glossary

Activation code

Is a unique key that can be bought from retail and used to activate a specific product or service. An activation code enables the activation of a valid subscription for a certain period of time and number devices and can also be used to extend a subscription with the condition to be generated for the same product or service.

ActiveX

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

Advanced persistent threat

Advanced persistent threat (APT) exploits vulnerabilities of systems to steal important information to deliver it to the source. Big groups such as organizations, companies, or governments, are targeted by this malware.

The objective of an advanced persistent threat is to remain undetected for a long time being able to monitor and gather important information without damaging the targeted machines. The method used to inject the virus into the network is through a PDF file or an Office document that look harmless so that every user can run the files.

Adware

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

Archive

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

Backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

Boot sector

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

Boot virus

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

Browser

Short for Web browser, a software application used to locate and display Web pages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

Command line

In a command line interface, the user types commands in the space provided directly on the screen using command language.

Cookie

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

Disk drive

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

Download

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

E-mail

Electronic mail. A service that sends messages on computers via local or global networks.

Events

An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

False positive
Occurs when a scanner identifies a file as infected when in fact it is not.

Filename extension
The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

Heuristic
A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

IP
Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

Java applet
A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

Keylogger
A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However,

they are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

Macro virus

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

Mail client

An e-mail client is an application that enables you to send and receive e-mail.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

Non-heuristic

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

Packed programs

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

Path

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Photon

Photon is an innovative non-intrusive Bitdefender technology, designed to minimize the performance impact of antivirus protection. By monitoring your PC's activity in the background, it creates usage patterns that help optimize booting and scanning processes.

Polymorphic virus

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

Port

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Ransomware

Ransomware is a malicious program that tries to make money from users by locking their vulnerable systems. CryptoLocker, CryptoWall,

and TeslaWall, are only some variants that hunt personal systems of users.

The infection can be spread by accessing spam e-mail, downloading e-mail attachments, or installing applications, without letting the user know about what is happening on his system. Daily users and companies are targeted by ransomware hackers.

Report file

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

Rootkit

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

Script

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

Spam

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

Spyware

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Startup items

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

Subscription

Purchase agreement that gives the user the right to use a particular product or service on a specific number of devices and for a certain period of time. An expired subscription can be automatically renewed using the information provided by the user at the first purchase.

System tray

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem,

volume, and more. Double click or right-click an icon to view and access the details and controls.

TCP/IP

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

Trojan

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

Update

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more

dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus signature

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

Worm

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.